(19)日本国特許庁（ＪＰ） (12)公開特許公報（Ａ） (11)特許出願公開番号

特開平11－234262

(43)公開日 平成11年(1999)８月27日

(51)Int.Cl.⁶		識別記号	FI		
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｇ
					５５０Ｃ
Ｇ０６Ｋ	19/10		Ｇ０９Ｃ	1/00	６４０Ｅ
Ｇ０９Ｃ	1/00	６４０			６６０Ｄ

審査請求 未請求 請求項の数10 ＯＬ （全 32 頁） 最終頁に続く

(21)出願番号 特願平10－27326

(22)出願日 平成10年(1998)２月９日

(71)出願人 000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者 中津山 恒
神奈川県足柄上郡中井町境430 グリーンテクなかい 富士ゼロックス株式会社内

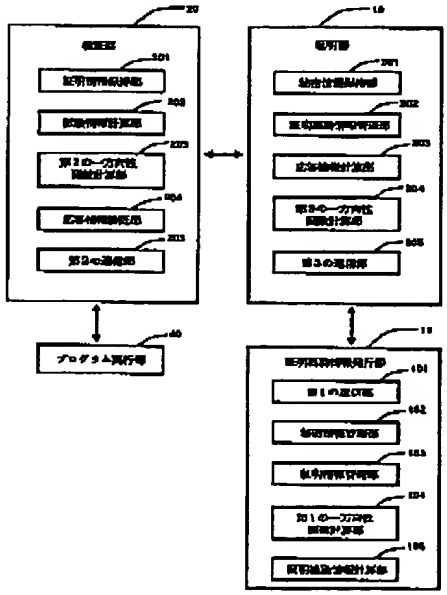
(74)代理人 弁理士 澤田 俊夫

(54)【発明の名称】 利用資格検証装置

(57)【要約】

【課題】 ＣＰＵパワー・メモリの少ない装置で高速に認証を行なう。

【解決手段】 検証器２０の試験情報計算部２０２は、乱数を生成し、乱数と権利の識別情報とを併せて試験情報として証明器３０へ伝達する。証明器３０の第３の一方向性関数計算部３０４は、秘密情報保持部３０１が保持する秘密情報と試験情報の権利識別情報とに対し、一方向性関数を適用する。応答情報計算部３０３は、一方向性関数の計算結果と証明補助情報とを演算し、証明情報を求める。さらに第３の一方向性関数計算部３０４は、証明情報と試験情報に含まれる乱数とに対し、一方向性関数を適用し、応答情報とし、検証器２０に返す。検証器２０の第２の一方向性関数計算部２０３は、証明情報と試験情報の乱数に対し、一方向性関数を適用する。応答情報検証器２０４は、一方向性関数の適用結果と、応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。



【特許請求の範囲】

【請求項1】 証明補助情報発行部、検証部および証明部を含み、利用資格を検証する利用資格検証装置において、

前記証明補助情報発行部は、利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、

秘密の情報を管理する秘密情報管理手段と、

少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第1の一方向性関数計算手段と、

前記秘密情報管理手段が管理する秘密情報と、前記第1の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、証明補助情報の計算の過程で情報を送受信する第1の通信手段とを有し、

前記検証部は、

証明情報を保持する証明情報保持手段と、

試験情報を計算する試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第2の一方向性関数計算手段と、

前記証明情報保持手段が保持する証明情報と、試験情報の一部もしくは全部をもとに得られる値に対し前記第2の一方向性計算手段を作用させた結果と応答情報が等しいか検査する応答情報検証手段と、

利用資格の認証の過程で情報を送受信する第2の通信手段とを有し、

前記証明部は、

秘密の情報を保持する秘密情報保持手段と、

応答情報の計算に用いる証明補助情報を管理する証明補助情報管理手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第3の一方向性関数計算手段と、

試験情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第3の一方向性関数計算手段を作用させて応答情報を計算する応答情報計算手段と、

利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第3の通信手段とを有することを特徴とする利用資格検証装置。

【請求項2】 証明補助情報発行部、検証部および証明部を含み、利用資格を検証する利用資格検証装置において、

前記証明補助情報発行部は、

利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、

少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する、第1の一方向性関数計算手段と、

前記秘密情報管理手段が管理する秘密情報と、前記第1の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、

証明補助情報の計算の過程で情報を送受信する第1の通信手段とを有し、

前記検証部は、

秘密の情報を保持する第1の秘密情報保持手段と、

証明補助情報を管理する第1の証明補助情報管理手段と、

試験情報を計算する試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な方向性関数を適用する第2の一方向性関数計算手段と、

前記第1の秘密情報保持手段が保持する秘密情報と、試験情報の一部もしくは全部をもとに得られる値に対し前記第2の一方向性計算手段を作用させた結果と応答情報が等しいか検査する応答情報検証手段と、

利用資格の認証の過程で情報を送受信する第2の通信手段とを有し、

前記証明部は、

秘密の情報を保持する第2の秘密情報保持手段と、

応答情報の計算に用いる証明補助情報を管理する第2の証明補助情報管理手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第3の一方向性関数計算手段と、

試験情報の一部もしくは全部と、前記第2の秘密情報保持手段が保持する秘密情報と、前記第2の証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第3の一方向性関数計算手段を作用させて応答情報を計算する応答情報計算手段と、

利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第3の通信手段とを有することを特徴とする利用資格検証装置。

【請求項3】 請求項1ないし請求項2の利用資格検証装置であって、

前記証明情報管理手段は、利用条件を示す情報である使用制限記述を証明情報と併せて管理し、

前記証明補助情報管理手段は、使用制限記述を証明補助情報と併せて管理し、

前記証明部で用いる証明補助情報および前記証明部で生成する応答情報の計算には使用制限記述を含むことを特徴とする利用資格検証装置。

【請求項4】 請求項1ないし請求項3の利用資格検証装置であって、復号手段を備え、利用資格があると判定した場合には、証明情報あるいは証明情報から得られる値を前記復号手段の復号鍵として用い、情報を復号することを特徴とする利用資格検証装置。

【請求項5】 請求項1ないし請求項4の利用資格検証装置であって、利用資格検証時の履歴を管理する履歴管

理手段を備え、証明情報保持手段あるいは第１の証明補助情報管理手段は、伝送情報を証明情報あるいは証明補助情報と併せて管理し、試験情報はさらに伝送情報を含み、利用資格検証時に前記伝送情報を履歴管理手段に格納することを特徴とする利用資格検証装置。

【請求項６】　証明補助情報発行部、検証部および証明部を含み、利用資格を検証する利用資格検証装置において、

前記証明補助情報発行部は、

利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、

秘密の情報を管理する秘密情報管理手段と、

少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第１の一方向性関数計算手段と、

前記秘密情報管理手段が管理する秘密情報と、前記第１の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、

証明補助情報の計算の過程で情報を送受信する第１の通信手段とを有し、

前記検証部は、

証明情報を保持する証明情報保持手段と、

第１の試験情報を計算する第１の試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第２の一方向性関数計算手段と、

受信した第２の試験情報に前記第２の一方向性関数計算手段を作用させ、第１の応答情報を計算する第１の応答情報計算手段と、

前記証明情報保持手段が保持する証明情報と、第１の試験情報の一部もしくは全部をもとに得られる値に対し前記第２の一方向性計算手段を作用させた結果と第２の応答情報が等しいか検査する第１の応答情報検証手段と、

利用資格の認証の過程で情報を送受信する第２の通信手段とを有し、

前記証明部は、

秘密の情報を保持する秘密情報保持手段と、

応答情報の計算に用いる証明補助情報を管理する証明補助情報管理手段と、

証明補助情報に対応する内部状態を管理する内部状態管理手段と、

試験情報を計算する第２の試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第３の一方向性関数計算手段と、

受信した情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させて第２の応答情報を計算する第２の応答情報計算手段と、

第２の試験情報を計算する第２の試験情報計算手段と、

第１の応答情報、および第２の試験情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させた結果と応答情報が等しいか検査する第２の応答情報検証手段と、

利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第３の通信手段とを有することを特徴とする利用資格検証装置。

【請求項７】　証明補助情報発行部、検証部および証明部を含み、利用資格を検証する利用資格検証装置において、

前記証明補助情報発行部は、

利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、

少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第１の一方向性関数計算手段と、

前記秘密情報管理手段が管理する秘密情報と、前記第１の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、

証明補助情報の計算の過程で情報を送受信する第１の通信手段とを有し、

前記検証部は、

秘密の情報を保持する第１の秘密情報保持手段と、

証明補助情報を管理する第１の証明補助情報管理手段と、

第１の試験情報を計算する第１の試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第２の一方向性関数計算手段と、

受信した第２の試験情報に前記第２の一方向性関数計算手段を作用させ、第１の応答情報を計算する第１の応答情報計算手段と、

前記証明情報保持手段が保持する証明情報と、第１の試験情報の一部もしくは全部をもとに得られる値に対し前記第２の一方向性計算手段を作用させた結果と第２の応答情報が等しいか検査する第１の応答情報検証手段と、

利用資格の認証の過程で情報を送受信する第２の通信手段とを有し、

前記証明部は、

秘密の情報を保持する第２の秘密情報保持手段と、

応答情報の作成に用いる証明補助情報を管理する第２の証明補助情報管理手段と、

証明補助情報に対応する内部状態を管理する内部状態管理手段と、

試験情報を計算する第２の試験情報計算手段と、

逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第３の一方向性関数計算手段と、

受信した情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させて第２の応答情報を計算する第２の応答情報計算手段と、

第２の試験情報を計算する第２の試験情報計算手段と、第１の応答情報、および第２の試験情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させた結果と応答情報が等しいか検査する第２の応答情報検証手段と、

利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第３の通信手段とを有する特徴とする利用資格検証装置。

【請求項８】　請求項６ないし請求項７の利用資格検証装置であって、証明情報管理手段は、利用条件を示す情報である使用制限記述を証明情報と併せて管理し、証明補助情報管理手段、使用制限記述を証明補助情報と併せて管理し、証明部で用いる証明補助情報および証明部で生成される応答情報の計算には使用制限記述を含むことを特徴とする利用資格検証装置。

【請求項９】　請求項６ないし請求項８の利用資格検証装置であって、復号手段を備え、利用資格があると判定した場合には、証明情報あるいは証明情報から得られる値を前記復号手段の復号鍵として用い、情報を復号することを特徴とする利用資格検証装置。

【請求項１０】　請求項６ないし請求項９の利用資格検証装置であって、利用資格検証時の履歴を管理する履歴管理手段を備え、証明情報保持手段あるいは第１の証明補助情報管理手段は、伝達情報を証明情報あるいは証明補助情報と併せて管理し、試験情報はさらに伝達情報を含み、利用資格検証時に前記伝達情報を履歴管理手段に格納することを特徴とする利用資格検証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、利用資格を検証する利用資格検証装置に関する。

【０００２】

【従来の技術】ネットワークの進展につれ、ソフトウェアやマルチメディアデータなどのデジタル情報で表現された知的財産が飛躍的に増大している。そして、デジタル情報は簡単に複製することがで、また不正にコピーしたとしても一切痕跡が残らない。このため、デジタル情報に関する著作権の保護が問題となっている。

【０００３】利用の権利を表すものとして日常的に用いているものにチケットがあり、チケットのデジタル化も試みられている。しかしながら、前述の著作権保護と同様の問題がある。

【０００４】ソフトウェアの利用資格を検証する従来の技術として、米国特許５，５８６，１８６号明細書で開示されている技術がある。（以下、従来技術と呼ぶ。）この技術はソフトウェアのアクセス制御を実現するものであるが、暗号化されたソフトウェアを復号する代わりに、暗号化された所与の情報が正しく復号されることで利用資格を確認することにより、チケットのデジタル化にも用いることができる。

【０００５】従来技術では、ソフトウェアを暗号化した状態で配布しておき、利用者が該ソフトウェアの利用を希望するときには、復号するための情報（利用者鍵）をソフトウェアベンダから購入する方法を採っている。暗号化にはＲＳＡ（Ｒｉｖｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）公開鍵暗号を用いており、利用者鍵としてＲＳＡ公開鍵対の秘密鍵と利用者識別情報に所定の演算を行なって得られる値を使用する。

【０００６】

【従来技術の問題点】従来技術は、ＲＳＡベースの認証方式であるため、計算量が多い。ＢｒｕｃｅＳｃｈｎｅｉｅｒ，Ａｐｐｌｉｅｄ　Ｃｒｙｐｔｏｇｒａｐｈｙ（Ｓｅｃｏｎｄ　Ｅｄｉｔｉｏｎ），Ｗｉｌｅｙ，１９９６によれば、ワークステーション（ＳＰＡＲＣ２）で、法数１０２４ビット・公開鍵８ビットのＲＳＡ暗号系を使って１０２４ビットのデータを処理する時間は、署名が０．９７秒、検証が０．０８秒かかっている。このため、ＩＣカードのような、ワークステーションと比較してはるかにＣＰＵパワー・メモリが少ない装置では、認証のために時間が掛かるという問題がある。

【０００７】

【発明が解決しようとする課題】本発明は上記の問題に鑑みてなされたもので、ＩＣカードのようにＣＰＵパワー・メモリの少ない装置でも高速に認証が可能な利用資格検証装置の実現を課題とする。

【０００８】

【課題を解決する手段】前記課題を解決するため、請求項１の利用資格検証装置は、証明補助情報発行部、検証部および証明部を有する。そして、前記証明補助情報発行部は、利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、証明補助情報の計算に用いる第１の一方向性関数計算手段と、証明補助情報を計算する証明補助情報計算手段と、第１の通信手段とを有する。また、前記検証部は、証明情報を保持する証明情報保持手段と、試験情報を計算する試験情報計算手段と、第２の一方向性関数計算手段と、応答情報を検証する応答情報検証手段と、第２の通信手段とを有する。さらに、前記証明部は、秘密情報を保持する秘密情報保持手段と、証明補助情報を管理する証明補助情報管理手段と、第３の一方向性関数計算手段と、応答情報を計算する応答情報計算手段と、第３の通信手段とを有する。

【０００９】また、請求項２の利用資格検証装置は、証

明補助情報発行部、検証部および証明部を有する。そして、前記証明補助情報発行部は、証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、証明補助情報の計算に用いる第１の一方向性関数計算手段と、証明補助情報を計算する証明補助情報計算手段と、第１の通信手段とを有する。また、前記検証部は、秘密情報を保持する第１の秘密情報保持手段と、証明補助情報を管理する第１の証明補助情報管理手段と、試験情報を計算する試験情報計算手段と、第２の一方向性関数計算手段と、応答情報を検証する応答情報検証手段と、第２の通信手段とを有する。さらに、前記証明部は、秘密情報を保持する第２の秘密情報保持手段と、証明補助情報を管理する第２の証明補助情報管理手段と、第３の一方向性関数計算手段と、応答情報を計算する応答情報計算手段と、第３の通信手段とを有する。

【００１０】請求項３の利用資格検証装置は、請求項１ないし請求項２の利用資格検証装置であって、証明情報管理手段は、利用条件を示す情報である使用制限記述を証明情報と併せて管理し、証明補助情報管理手段は、使用制限記述を証明補助情報と併せて管理し、前記証明部で用いる証明補助情報および前記証明部で生成される応答情報の計算には使用制限記述を含む。

【００１１】請求項４の利用資格検証装置は、請求項１ないし請求項３の利用資格検証装置であって、復号手段を備え、利用資格があると判定した場合には、証明情報あるいは証明情報から得られる値を前記復号手段の復号鍵として用い、情報を復号する。

【００１２】請求項５の利用資格検証装置は、請求項１ないし請求項４の利用資格検証装置であって、利用資格検証時の履歴を管理する履歴管理手段を備え、第１の証明補助情報管理手段は、伝達情報を証明補助情報と併せて管理し、試験情報はさらに伝達情報を含み、利用資格検証時に前記伝達情報を履歴管理手段に格納する。

【００１３】請求項６の利用資格検証装置は、証明補助情報発行部、検証部および証明部を有する。そして、前記証明補助情報発行部は、利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第１の一方向性関数計算手段と、前記秘密情報管理手段が管理する秘密情報と、前記第１の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、証明補助情報の計算の過程で情報を送受信する第１の通信手段とを有する。また、前記検証部は、証明情報を保持する証明情報保持手段と、第１の試験情報を計算する第１の試験情報計算手段と、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第２の一方向性関数計算手段と、受信した第２の試験情報に前記第２の一方向性関数計算手段を作用させ、第１の応答情報を計算する第１の応答情報計算手段と、前記証明情報保持手段が保持する証明情報と、第１の試験情報の一部もしくは全部をもとに得られる値に対し前記第２の一方向性計算手段を作用させた結果と第２の応答情報が等しいか検査する第１の応答情報検証手段と、利用資格の認証の過程で情報を送受信する第２の通信手段とを有する。さらに、前記証明部は、秘密の情報を保持する秘密情報保持手段と、応答情報の作成に用いる証明補助情報を管理する証明補助情報管理手段と、証明補助情報に対応する内部状態を管理する内部状態管理手段と、試験情報を計算する第２の試験情報計算手段と、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第３の一方向性関数計算手段と、受信した情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させて第２の応答情報を計算する第２の応答情報計算手段と、第２の試験情報を計算する第２の試験情報計算手段と、第１の応答情報、および第２の試験情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させた結果と応答情報が等しいか検査する第２の応答情報検証手段と、利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第３の通信手段とを有している。

【００１４】請求項７の利用資格検証装置は、証明補助情報発行部、検証部および証明部を有する。そして、前記証明情報発行部は、利用資格の認証の際に用いる証明情報を管理する証明情報管理手段と、秘密の情報を管理する秘密情報管理手段と、少なくとも前記秘密情報管理手段が管理する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第１の一方向性関数計算手段と、前記秘密情報管理手段が管理する秘密情報と、前記第１の一方向性関数計算手段の計算結果をもとに証明補助情報を計算する証明補助情報計算手段と、証明補助情報の計算の過程で情報を送受信する第１の通信手段と、秘密の情報を保持する第１の秘密情報保持手段と、証明補助情報を管理する第１の証明補助情報管理手段と、第１の試験情報を計算する第１の試験情報計算手段と、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第２の一方向性関数計算手段と、受信した第２の試験情報に前記第２の一方向性関数計算手段を作用させ、第１の応答情報を計算する第１の応答情報計算手段と、前記証明情報保持手段が保持する証明情報と、第１の試験情報の一部もしくは全部をもとに得られる値に対し前記第２の一方向性計算手段を作用させた結果と第２の応答情報が等しいか検査する第１の応答情報検証手段と、利用資格の認証

の過程で情報を送受信する第２の通信手段とを有する。さらに、前記証明部は、秘密の情報を保持する第２の秘密情報保持手段と、応答情報の作成に用いる証明補助情報を管理する第２の証明補助情報管理手段と、証明補助情報に対応する内部状態を管理する内部状態管理手段と、試験情報を計算する第２の試験情報計算手段と、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する第３の一方向性関数計算手段と、受信した情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させて第２の応答情報を計算する第２の応答情報計算手段と、第２の試験情報を計算する第２の試験情報計算手段と、第１の応答情報、および第２の試験情報の一部もしくは全部と、前記秘密情報保持手段が保持する秘密情報と、前記証明補助情報管理手段が管理する証明補助情報をもとに得られる値に、前記第３の一方向性関数計算手段を作用させた結果と応答情報が等しいか検査する第２の応答情報検証手段と、利用資格の認証の過程および証明補助情報計算の過程で情報を送受信する第３の通信手段とを有している。

【００１５】請求項８の利用資格検証装置は、請求項６ないし請求項７の利用資格検証装置であって、証明情報管理手段は、利用条件を示す情報である使用制限記述を証明情報と併せて管理し、証明補助情報管理手段は、使用制限記述を証明補助情報と併せて管理し、前記証明部で用いる証明補助情報および前記証明部で生成される応答情報の計算には使用制限記述を含む。

【００１６】請求項９の利用資格検証装置は、請求項６ないし請求項８の利用資格検証装置であって、復号手段を備え、利用資格があると判定した場合には、証明情報あるいは証明情報から得られる値を前記復号手段の復号鍵として用い、情報を復号する。

【００１７】請求項１０の利用資格検証装置は、請求項６ないし請求項９の利用資格検証装置であって、利用資格検証時の履歴を管理する履歴管理手段を備え、第１の証明補助情報管理手段は、伝送情報を証明補助情報と併せて管理し、試験情報はさらに伝達情報を含み、利用資格検証時に前記伝送情報を履歴管理手段に格納する。

【００１８】

【作用】本発明の利用資格検証装置は、証明補助情報の発行と、利用資格の検証を行う。

【００１９】証明補助情報の発行では、各手段はいずれの請求項の利用資格検証装置も以下の作用をする。

【００２０】第１の通信手段で、秘密情報保持手段を有するどの機器に対して、どのような権利を発行するかを識別するための情報を受信する。該権利を期間などで制限する使用制限記述がある場合には、このとき使用制限記述が併せて指定される。

【００２１】秘密情報管理手段は、機器を識別する情報から、該機器の秘密情報保持手段が保持する秘密情報を検索する。

【００２２】証明情報管理手段は、権利を識別する情報から、該権利に対応する証明情報を検索する。第１の一方向性関数計算手段は、少なくとも該秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。使用制限記述が存在する場合には、使用制限記述も含めて一方向性関数を適用する。

【００２３】証明補助情報計算手段は、該証明情報と、一方向性関数を適用した結果得られる値をもとに、証明補助情報を計算する。

【００２４】該証明補助情報は、第１の通信手段から送信され、該機器の通信手段へと伝送されて、該機器の証明補助情報管理手段に格納される。

【００２５】請求項１の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００２６】試験情報計算手段は、乱数を生成し、該乱数と証明情報保持手段が保持する権利の識別情報を併せて試験情報とする。

【００２７】該試験情報は、第２の通信手段から第３の通信手段へと伝達される。証明補助情報管理手段は、該試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【００２８】第３の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００２９】応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。第３の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、応答情報とする。

【００３０】第３の通信手段は、応答情報を第２の通信手段へ伝達する。

【００３１】第２の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００３２】応答情報検証部は、前記一方向性関数の適用結果と、該応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【００３３】請求項２の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００３４】利用資格の検証に先立ち、第２の通信手段から権利の識別情報を入力するか、事前に定められた規則にしたがって計算することにより、どの権利を検証するかを決定する。

【００３５】試験情報計算手段は、乱数を生成し、該乱数と該権利の識別情報を併せて試験情報とする。

【００３６】該試験情報は、第２の通信手段から第３の通信手段へと伝達される。第２の証明補助情報管理手段は、該試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【００３７】第３の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００３８】応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。

【００３９】第３の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、応答情報とする。

【００４０】第３の通信手段は、応答情報を第２の通信手段へ伝達する。

【００４１】第２の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００４２】応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。

【００４３】第２の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００４４】応答情報検証部は、前記一方向性関数の適用結果と、該応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【００４５】請求項３の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００４６】この利用資格検証装置は、請求項１ないし請求項２の利用資格検証装置と同様の手段を備える。

【００４７】応答情報の計算に用いる証明補助情報を管理する証明補助情報管理手段は、使用限記述を証明補助情報と併せて管理し、権利の識別情報から証明補助情報を検索する際、使用制限記述も同時に検索する。

【００４８】第３の一方向性関数計算手段は、該権利識別情報、該使用制限記述、および秘密情報保持手段が保持する秘密情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００４９】応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。第３の一方向性関数計算手段は、該証明情報、該試験情報の乱数、および該使用制限記述に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。該使用制限記述とここで得られた値とを併せて、応答情報とする。

【００５０】応答情報検証手段は、証明情報、該試験情報の乱数、該応答情報の使用制限記述に対して第１の一方向性関数計算手段を適用した値と、該応答情報の使用制限記述以外の情報が一致し、かつ使用制限記述が所定の条件を満たす場合に限り利用資格があるものと判定する。（応答情報計算手段で使用制限記述が所定の条件を満たすか判定する方法もある。）

請求項４の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００５１】この利用資格検証装置は、請求項１ないし請求項３の利用資格検証装置と同様の手段を備える。

【００５２】応答情報検証手段で、利用資格があるものと判定された場合には、復号手段により証明情報あるいは証明情報から得られる値を前記復号手段の復号鍵として用い、情報を復号する。

【００５３】請求項５の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００５４】この利用資格検証装置は、請求項１ないし請求項４の利用資格検証装置と同様の手段を備える。

【００５５】証明情報保持手段あるいは第１の証明補助情報管理手段は、伝達情報を証明情報あるいは証明補助情報と併せて管理する。

【００５６】試験情報は、さらに該伝達情報を含む。

【００５７】利用資格検証時に前記伝達情報を履歴管理手段に格納する。

【００５８】請求項６の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００５９】第１の試験情報計算手段は、第１の乱数を生成し、少なくとも該乱数と証明情報保持手段が保持する権利の識別情報を併せて試験情報とする。

【００６０】該試験情報は、第２の通信手段から第３の通信手段へと伝達される。

【００６１】第２の試験情報計算手段は、第２の乱数を生成して、これを第２の試験情報とする。

【００６２】第３の通信手段は、第２の試験情報を第２の通信手段に伝達する。第１の応答情報計算手段は、少なくとも第２の試験情報を第２の一方向性関数計算手段に入力し、ここで得られた値を含む情報を第１の応答情報とする。

【００６３】第１の応答情報は、第２の通信手段から第３の通信手段へと伝達される。第３の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００６４】証明補助情報管理手段は、該試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【００６５】第２の応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。次いで、第１の応答情報が、第２の試験情報と該証明情報を含む情報に対し、第３の一方向性関数

計算手段を適用して得られる値を比較する。

【００６６】値が所定の関係を満たさなければ意味のない値を生成して第２の応答情報とし、所定の関係を満たせば、後述の内部状態の変更と応答情報の計算を行う。

【００６７】内部状態管理手段は、該権利識別情報に対応する内部状態を検索し、第１の試験情報もしくは第１の応答情報で伝達された情報に応じて、該内部状態を変更する。

【００６８】第３の一方向性関数計算手段は、該証明情報と、第１の試験情報に含まれる第１の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００６９】第２の応答情報計算手段は、この値を第２の応答情報とする。

【００７０】第３の通信手段は、応答情報を第２の通信手段へ伝達する。

【００７１】第２の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００７２】応答情報検証部は、前記一方向性関数の適用結果と、該応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【００７３】請求項７の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００７４】利用資格の検証に先立ち、第２の通信手段から権利の識別情報を入力するか、事前に定められた規則にしたがって計算することにより、どの権利を検証するかを決定する。

【００７５】試験情報計算手段は、乱数を生成し、該乱数と該権利の識別情報を併せて試験情報とする。

【００７６】該試験情報は、第２の通信手段から第３の通信手段へと伝達される。第１の証明補助情報管理手段は、該試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【００７７】第１の試験情報計算手段は、第１の乱数を生成し、少なくとも該乱数と証明情報保持手段が保持する権利の識別情報を併せて試験情報とする。該試験情報は、第２の通信手段から第３の通信手段へと伝達される。第２の試験情報計算手段は、第２の乱数を生成して、これを第２の試験情報とする。

【００７８】第３の通信手段は、第２の試験情報を第２の通信手段に伝達する。第２の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００７９】第１の応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。

【００８０】第１の応答情報計算手段は、少なくとも該証明情報と第２の試験情報を第２の一方向性関数計算手段に入力し、ここで得られた値を含む情報を第１の応答情報とする。

【００８１】第１の応答情報は、第２の通信手段から第３の通信手段へと伝達される。第３の一方向性関数計算手段は、秘密情報保持手段が保持する秘密情報と該権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００８２】証明補助情報管理手段は、該試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【００８３】第２の応答情報計算手段は、前記の一方向性関数の計算結果と該証明補助情報とを演算し、証明情報を求める。次いで、第１の応答情報が、第２の試験情報と該証明情報を含む情報に対し、第３の一方向性関数計算手段を適用して得られる値を比較する。

【００８４】値が所定の関係を満たさなければ意味のない値を生成して第２の応答情報とし、所定の関係を満たせば、後述の内部状態の変更と応答情報の計算を行う。

【００８５】内部状態管理手段は、該権利識別情報に対応する内部状態を検索し、第１の試験情報もしくは第１の応答情報で伝達された情報に応じて、該内部状態を変更する。

【００８６】第３の一方向性関数計算手段は、該証明情報と、第１の試験情報に含まれる第１の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００８７】第２の応答情報計算手段は、この値を第２の応答情報とする。

【００８８】第３の通信手段は、応答情報を第２の通信手段へ伝達する。

【００８９】第２の一方向性関数計算手段は、該証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【００９０】応答情報検証部は、前記一方向性関数の適用結果と、該応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【００９１】請求項１０の利用資格検証装置での利用資格の検証における作用は、以下の通りである。

【００９２】この利用資格検証装置は、請求項６ないし請求項９の利用資格検証装置と同様の手段を備える。

【００９３】証明情報保持手段あるいは第１の証明補助情報管理手段は、伝達情報を証明情報あるいは証明補助情報と併せて管理する。

【００９４】第１の試験情報もしくは第１の応答情報は、さらに該伝達情報を含む。

【００９５】利用資格検証時に前記伝達情報を履歴管理手段に格納する。

【００９６】

【発明の実施の態様】以下に述べる実施例の利用資格検証装置は、いずれも証明補助情報発行器、検証器、証明

器の３つの要素からなる。

【００９７】証明補助情報発行器は、利用資格の検証の過程で用いる証明補助情報を発行する。

【００９８】検証器と証明器は対話証明を行って、利用資格の有無を検証する。対話証明の過程では、公開鍵暗号系と比べて計算量がはるかに少ない、ＭＤ５やＳＨＡなどの一方向性関数を用いる。以下の実施例では、一方向性関数として複数の引数を取るものを用いるが、各引数のビット列を連結することにより、ＭＤ５やＳＨＡを

第１の実施例	請求項１	図１
第２の実施例	請求項２	図２
第３の実施例	請求項３	図２
第４の実施例	請求項４	図３
第５の実施例	請求項５	図４、図９
第６の実施例	請求項６	図５
第７の実施例	請求項７	図６
第８の実施例	請求項８	図６
第９の実施例	請求項９	図７
第１０の実施例	請求項１０	図８、図１０

【０１０１】［第１の実施例］以下、第１の実施例について説明する。この実施例は、一方向性関数を用いて基本的な対話認証を行なうものである。

【０１０２】図１は、第１の実施例の構成を示しており、この図において、利用資格検証装置は、証明補助情報発行器１０、検証器２０および証明器３０を含んでいる。証明補助情報発行器１０は証明器２０に証明補助情報を発行する。証明器３０は、この証明補助情報を利用して検証器２０との間で対話認証を行い。認証が成功すると例えばプログラム実行部４０がプログラムを実行するようになっている。

【０１０３】証明補助情報発行器１０は、第１の通信部１０１、秘密情報管理部１０２、証明情報管理部１０３、第１の一方向性計算部１０４、証明補助情報計算部１０５を含んで構成されている。

【０１０４】証明補助情報発行器１０の処理の流れは図１１に示されている。

【０１０５】この証明補助情報発行器１０は、証明器３０からの要求に基づいて証明補助情報の発行を行なう。第１の通信部１０１は、証明器３０から、証明装置３０の識別情報や、どのような権利を発行するかを識別するための情報を受信する（図１１のＳ１１、Ｓ１２）。秘密情報管理部１０２は、証明装置３０を識別する情報から、証明装置３０が保持する秘密情報を検索する（Ｓ１３）。証明情報管理部１０３は、権利を識別する情報から、該権利に対応する証明情報（Ｋ）を検索する。第１の一方向性関数計算部１０４は、少なくとも秘密情報と権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。証明補助情報計算部１０５は、証明情報と、一方向性関数を適用した結果得られる値をもとに、証明補助情報を計算する（Ｓ１４）。この証明補助情報は、第１の通信部１０１から証明器３０に送信される（Ｓ１５）。

【０１０６】検証器２０は、証明情報保持部２０１、試験情報計算部２０２、第２の一方向性関数計算部２０３、応答情報検証器２０４および第２の通信部２０５を含んで構成されている。

【０１０７】検証器２０は、証明器３０に試験情報を送り、証明器３０から返される証明情報を検証して証明装置との間で対話認証を行なう。

【０１０８】検証器２０の処理の流れは図１２に示されている。

【０１０９】証明情報保持部２０１は、権利の識別情報を保持している。試験情報計算部２０２は、乱数を生成し、乱数と証明情報保持部２０１が保持する権利の識別情報とを併せて試験情報とする（図１２のＳ２１）。この試験情報は、第２の通信部２０５から証明器３０の第３の通信部３０５へと伝達される（Ｓ２２）。また第２の通信部２０５は証明器３０から返される応答情報を受信する（Ｓ２３）。第２の一方向性関数計算部２０３は、証明情報と該試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。応答情報検証器２０４は、一方向性関数の適用結果と、応答情報とを比較し、一致する場合に限り利用資格があるものと判定する（Ｓ２４、Ｓ２５）。

【０１１０】証明器３０は、秘密情報保持部３０１、証明補助情報管理部３０２、応答情報計算部３０３、第３の一方向性関数計算部３０４および第３の通信部３０５を含んで構成されている。

【０１１１】証明器３０は、検証器２０から送られてくる試験情報に対して所定の計算を施して応答情報を生成し、検証器２０に返す。

用いることができる。

【００９９】なお、以下説明する利用者資格検証装置の実施例と請求項との対応関係は以下のとおりであり、各実施例を対応する図を参照して説明する。なお、図１～図８は各実施例の構成を示しており、図９および図１０は動作を示している。

【０１００】

【表１】

【０１１２】証明器３０の処理の流れは図１３に示されている。

【０１１３】試験情報は、第２の通信部２０５から第３の通信部３０５へと伝達される（Ｓ３１）。

【０１１４】秘密情報保持部３０１は、証明器３０に固有の秘密情報を保持している。証明補助情報管理部３０２は、試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する（Ｓ３２）。証明補助情報は予め証明補助情報発行器１０から入手している。第３の一方向性関数計算部３０４は、秘密情報保持部３０１が保持する秘密情報と試験情報に含まれる権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する（Ｓ３３）。応答情報計算部３０３は、一方向性関数の計算結果と証明補助情報とを演算し、証明情報を求める。さらに第３の一方向性関数計算部３０４は、証明情報と試験情報に含まれる乱数とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、応答情報とする。この応答情報は第３の通信部３０５を介して検証器２０の第２の通信部２０５に送られる（Ｓ３４、Ｓ３５）。

【０１１５】以下、第１の実施例の認証のプロトコルについて詳細に説明する。

【０１１６】第１の実施例では、証明補助情報ｔを以下のように定める。

【０１１７】

【数１】ｔ＝Ｋ－ｆ（ｄ，ｎ）

ここで、Ｋは証明情報、ｆは一方向性関数、ｄは秘密情報、ｎは検証すべき権利を識別する情報である。　検証器２０から証明器３０に送る試験情報Ｃは、ｒを乱数として、

【０１１８】

【数２】Ｃ＝（ｎ，ｒ）である。

【０１１９】証明器３０は、以下の計算により応答情報Ｒを求める。

【０１２０】

【数３】Ｒ＝ｆ（ｔ＋ｆ（ｄ，ｎ），ｒ）

証明器３０が、正しい証明補助情報ｔを保持している場合には、

【０１２１】

【数４】ｔ＋ｆ（ｄ，ｎ）＝Ｋ－ｆ（ｄ，ｎ）＋ｆ（ｄ，ｎ）＝Ｋ

となって、証明情報Ｋを復元でき、

【０１２２】

【数５】Ｒ＝ｆ（Ｋ，ｒ）

となる。

【０１２３】検証器２０はｆ（Ｋ，ｒ）を求めて応答情報Ｒと比較し、両者が等しい場合に限り、証明器が利用資格を有するものと判定する。

【０１２４】［第２の実施例］つぎに第２の実施例について説明する。この実施例は、認証対象の権利が複数あり、どの権利について認証するかを予め決めるようになっている。どの権利を認証するかは、権利の識別情報を入力したり、予め定められた規則で計算を行なって決定する。一方向性関数を用いる認証手法の基本は第１の実施例と同様である。

【０１２５】図２は第２の実施例の構成を示しており、この図において、図１と対応する箇所には対応する符号を付した。

【０１２６】この実施例の証明補助情報発行器１０は、検証器１０および証明器２０の要求にそれぞれ応答して対応する証明補助情報を発行する。

【０１２７】検証器２０は、第１の秘密情報保持部２０６および第１の証明補助情報管理部２０７を有している。証明器３０は、第２の秘密情報保持部３０６および第２の証明補助情報管理部３０７を有している。

【０１２８】まず、利用資格の検証に先立ち、第２の通信部２０５を介して権利の識別情報が入力され、どの権利を検証するかが決定される。この決定は、事前に定められた規則にしたがって計算することにより、行なってもよい。

【０１２９】試験情報計算部２０２は、乱数を生成し、乱数と権利の識別情報を併せて試験情報とする。この試験情報は、第２の通信部２０５から証明器３０の第３の通信部３０５へと伝達される。

【０１３０】証明器３０の第２の証明補助情報管理部３０７は、試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。そして第３の一方向性関数計算部３０４は、第２の秘密情報保持部３０６が保持する秘密情報と権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。さらに、応答情報計算部３０３は、一方向性関数の計算結果と証明補助情報とを演算し、証明情報を求める。第３の一方向性関数計算部３０４は、さらに、証明情報と該試験情報の乱数とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、応答情報とする。この応答情報は第３の通信部３０５および第２の通信部２０５を介して検証器２０に送られる。

【０１３１】検証器２０の第２の一方向性関数計算部２０３は、第１の秘密情報保持部２０６が保持する秘密情報と権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。そして一方向性関数の計算結果と証明補助情報とに対して所定の演算が行なわれ、証明情報が求められる。第２の一方向性関数計算部２０３は、さらに証明情報と試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。応答情報検証器２０４は、一方向性関数の適用結果と、応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【０１３２】つぎに、第２の実施例の認証プロトコルについて詳細に説明する。

【０１３３】第２の実施例では、検証器の証明補助情報ｔｖと証明器の証明補助情報ｔｐを以下のように定める。

【０１３４】

【数６】

ｔｖ＝Ｋ－ｆ（ｄｖ，ｎ）

ｔｐ＝Ｋ－ｆ（ｄｐ，ｎ）

ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器２０の秘密情報、ｄｐは証明器３０の秘密情報、ｎは検証すべき権利を識別する情報である。

【０１３５】検証器２０から証明器３０に送る試験情報Ｃは、ｒを乱数として、

【０１３６】

【数７】Ｃ＝（ｎ，ｒ）

である。

【０１３７】証明器３０は、以下の計算により応答情報Ｒを求める。

【０１３８】

【数８】Ｒ＝ｆ（ｔｐ＋ｆ（ｄｐ，ｎ），ｒ）

証明器３０が、正しい証明補助情報ｔｐを保持している場合には、

【０１３９】

【数９】ｔｐ＋ｆ（ｄｐ，ｎ）＝Ｋ－ｆ（ｄｐ，ｎ）＋ｆ（ｄｐ，ｎ）＝Ｋ

となって、証明情報Ｋを復元でき、

【０１４０】

【数１０】Ｒ＝ｆ（Ｋ，ｒ）

となる。

【０１４１】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いでｆ（Ｋ，ｒ）を求めてＲと比較し、両者が等しい場合に限り、証明器が利用資格を有するものと判定する。

【０１４２】［第３の実施例］つぎに第３の実施例について説明する。この実施例は、第２の実施例においてさらに利用制限を導入するものである。

【０１４３】第３の実施例の構成自体は第２の実施例と同様であり、図２に示すとおりである。

【０１４４】以下、第３の実施例の認証プロトコルについて説明する。

【０１４５】第３の実施例では、検証器２０の証明補助情報ｔｖと証明器３０の証明補助情報ｔｐを以下のように定める。

【０１４６】

【数１１】

ｔｖ＝Ｋ－ｆ（ｄｖ，ｎ）

ｔｐ＝Ｋ－ｆ（ｄｐ，ｎ，Ｌ）

ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器２０の秘密情報、ｄｐは証明器３０の秘密情報、ｎは検証すべき権利を識別する情報、Ｌは使用制限記述である。使用制限記述Ｌは、たとえば使用期限を表すビット列である。

【０１４７】検証器２０から証明器３０に送る試験情報Ｃは、ｒを乱数として、

【０１４８】

【数１２】Ｃ＝（ｎ，ｒ）

である。

【０１４９】証明器３０は、以下の計算により応答情報Ｒを求める。

【０１５０】

【数１３】

Ｒ＝（Ｌ，ｆ（ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ），ｒ，Ｌ））

証明器３０が、正しい証明補助情報ｔｐを保持している場合には、

【０１５１】

【数１４】ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ）＝Ｋ－ｆ（ｄｐ，ｎ，Ｌ）＋ｆ（ｄｐ，ｎ，Ｌ）＝Ｋ

となって、証明情報Ｋを復元でき、

【０１５２】

【数１５】Ｒ＝（Ｌ，ｆ（Ｋ，ｒ，Ｌ））

となる。

【０１５３】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いでｆ（Ｋ，ｒ）を求めてＲと比較し、両者が等く、かつ使用制限記述Ｌが使用条件を満たす場合に限り、証明器３０が利用資格を有するものと判定する。

【０１５４】ここでは使用制限記述Ｌが使用条件を満たすか否かの判定を検証器２０で行うものとしたが、証明器３０で行うようにしてもよい。このときには、使用制限記述Ｌを応答情報に含めなくともよい。

【０１５５】［第４の実施例］つぎに第４の実施例について説明する。この実施例は、証明情報Ｋまたは証明情報から導出した値を鍵として暗号化された情報を復号するものである。

【０１５６】図３は、第４の実施例の構成を示しており、この図において図２と対応する箇所には対応する符号を付した。この実施例では、検証器２０に復号部２０８が付加されている。

【０１５７】第４の実施例で扱う情報および検証手順は第３の実施例と同じである。検証器２０の復号部２０８が、証明器３０が利用資格を有すると判定された場合に、証明情報Ｋあるいは Ｋを用いて計算可能な値を鍵として用い、暗号化された情報を復号する。

【０１５８】［第５の実施例］つぎに第５の実施例について説明する。この実施例は利用履歴を管理できるようにしたものである。

【０１５９】図４は、第５の実施例の構成を示しており、この図において、図３と対応する箇所には対応する符号を付した。図４においては、証明器３０に履歴管理

部３０８を設けている。

【０１６０】以下、第５の実施例の認証プロトコルについて説明する。

【０１６１】この認証手順は図９にも示す。第１～第４の実施例の各動作は第５の実施例に含まれているので第１～第４の実施例の動作も図９から理解できる。

【０１６２】以下、第５の実施例の認証プロトコルについて詳細に説明する。

【０１６３】第５の実施例では、検証器２０の証明補助情報ｔｖと証明器３０の証明補助情報ｔｐを以下のように定める。

【０１６４】

【数１６】

$tv=K-f(dv, n)$

$tp=K-f(dp, n, L)$

ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器２０の秘密情報、ｄｐは証明器３０の秘密情報、ｎは検証すべき権利を識別する情報、Ｌは使用制限記述である。使用制限記述Ｌは、たとえば使用期限を表すビット列である。

【０１６５】検証器２０は、$tv+f(dv, n)$を計算しＫを求める。

【０１６６】検証器２０から証明器３０に送る試験情報Ｃは、ｒを乱数として、

【０１６７】

【数１７】$C=(n, I, r, s)$

である。ここで、Ｉは検証器２０から証明器３０に伝達する情報、ｓは

【０１６８】

【数１８】$s=f(K, I, r)$

なる値である。　証明器３０は、以下の計算によりＫ'を求める。

【０１６９】

【数１９】$K'=tp+f(dp, n, L)$

次いで$f(K', I, r)$を計算し、ｓと比較する。ｓが一致した場合に限り、Ｉを含む情報を履歴保持部３０８に格納する。

【０１７０】証明器３０は、さらに、応答情報Ｒを求める。

【０１７１】

【数２０】

$R=(L, f(tp+f(dp, n, L), r, L))$

証明器３０が、正しい証明補助情報ｔｐを保持している場合には、

【０１７２】

【数２１】$tp+f(dp, n, L)=K-f(dp, n, L)+f(dp, n, L)=K$

となって、証明情報Ｋを復元でき、

【０１７３】

【数２２】$R=(L, f(K, r, L))$

となる。

【０１７４】次いで$f(K, r)$を求めてＲと比較し、両者が等く、かつＬが使用条件を満たす場合に限り、証明器が利用資格を有するものと判定する。

【０１７５】ここでは、使用制限記述Ｌが使用条件を満たすか否かの判定を検証器２０で行うものとしたが、証明器３０で行うようにしてもよい。

【０１７６】［第６の実施例］つぎに第６の実施例について説明する。第６の実施例は相互認証を行なって証明器３０の内部状態を変更できるようにしたものである。

【０１７７】図６は、第６の実施例の構成を示しており、この図において、図１と対応する箇所には対応する符号を付した。図６においては、検証器２０に第１の試験情報計算部２０９、第１の応答情報計算部２１０および第１の応答情報検証器２１１を設け、証明器３０に第２の試験情報計算部３０９、第２の応答情報計算部３１０、第２の応答情報検証器３１１および内部状態管理部３１２を設けている。

【０１７８】この実施例では、対話認証の過程で、お互いが認証を行い、検証器２０は復号等を行い、証明器３０は、復号等に対応する内部状態の変更を行なう。

【０１７９】この実施例の検証器２０および証明器３０の処理の流れはそれぞれ図１４および図１５に示されている。

【０１８０】検証器２０の第１の試験情報計算部２０９は、第１の乱数を生成し、少なくとも第１の乱数と証明情報保持部２０１が保持する権利の識別情報とを併せて試験情報とする（図１４のＳ４１）。この試験情報は、第２の通信部２０５から証明器３０の第３の通信部３０５へと伝達される（Ｓ４２、図１５のＳ５１）。

【０１８１】他方、第２の試験情報計算部３０９は、第２の乱数を生成して、これを第２の試験情報とし、第３の通信部３０５を介して検証器２０（第２の通信部２０５）へ送信する（Ｓ５２、Ｓ４３）。

【０１８２】検証器２０の第１の応答情報計算部２１０は、少なくとも第２の試験情報と、検証器２０から証明器３０に伝達した情報とを第２の一方向性関数計算部２０３に入力し、ここで得られた値と、伝達したい情報そのものとを含むように第１の応答情報を生成する。この第１の応答情報は、第２の通信部２０５から証明器３０の第３の通信部３０５へと伝達される（Ｓ４４、Ｓ５３）。

【０１８３】証明器３０の第３の一方向性関数計算部３０４は、秘密情報保持部３０１が保持する秘密情報と権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【０１８４】証明補助情報管理部３０２は、試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する（Ｓ５４）。

【０１８５】第２の応答情報計算部３１０は、一方向性

関数の計算結果と証明補助情報とを演算し、証明情報を求める。次いで、第２の試験情報と、証明情報を含む情報に対し、第３の一方向性関数計算部３０４を適用し、この結果得られた値と第１の応答情報（その一部）とを照合する（Ｓ５５、Ｓ５６）。値が所定の関係を満たさなければ意味のない値を生成して第２の応答情報とし、所定の関係を満たせば、後述の内部状態の変更と応答情報の計算を行う。

【０１８６】内部状態管理部３１２は、権利識別情報に対応する内部状態を検索し、第１の試験情報もしくは第１の応答情報で伝達された情報に応じて、内部状態を変更する。

【０１８７】第３の一方向性関数計算部３０４は、証明情報と、第１の試験情報に含まれる第１の乱数とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、第２の応答情報計算部３１１は、この値を第２の応答情報とする。第３の通信部３０５は、第２の応答情報を第２の検証器２０の通信部２０５へ伝達する（Ｓ５７、Ｓ５８、Ｓ４５））。

【０１８８】検証器２０の第２の一方向性関数計算部２０３は、証明情報と試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。第１の応答情報検証器２１１は、一方向性関数の適用結果と、第２の応答情報とを比較し、一致する場合に限り利用資格があるものと判定する（Ｓ４６、Ｓ４７）。

【０１８９】以下、第６の実施例の認証のプロトコルについて説明する。

【０１９０】第６の実施例では、証明補助情報ｔを以下のように定める。

【０１９１】

【数２３】ｔ＝Ｋ－ｆ（ｄ，ｎ）

ここで、Ｋは証明情報、ｆは一方向性関数、ｄは秘密情報、ｎは検証すべき権利を識別する情報である。

【０１９２】検証器２０から証明器３０に送る第１の試験情報Ｃ１は、ｒ１を乱数として、

【０１９３】

【数２４】Ｃ１＝（ｎ，ｒ１）

である。

【０１９４】証明器３０は、検証器２０へ第２の試験情報Ｃ２を送る。

【０１９５】

【数２５】Ｃ２＝ｒ２

ここで、ｒ２は乱数である。

【０１９６】検証器２０は、第１の応答情報Ｒ１を証明器３０へ送る。

【０１９７】

【数２６】Ｒ１＝（ｍ，ｆ（Ｋ，ｒ２，ｍ））

ここで、ｍは検証器２０から証明器３０へと伝達する情報である。ｍは、たとえば、利用の都度課金される額である。

【０１９８】証明器３０は、以下の計算によりＫ’を求める。

【０１９９】

【数２７】Ｋ’＝ｔｐ＋ｆ（ｄｐ，ｎ）

証明補助情報ｔｐが正しい場合には、Ｋ’は証明情報Ｋと一致する。

【０２００】証明器３０はｆ（Ｋ’，ｒ２，ｍ）を計算して、Ｒ１の第２項と比較する。両者が等しい場合には、検証器２０から伝達された情報ｍにしたがい、検証すべき権利に対応する内部状態を変更する。たとえば、ｍが利用の都度課金される額であれば、プリペイドの額を相応分だけ減じる。

【０２０１】次いで、証明器３０は第２の応答情報Ｒ２を求める。

【０２０２】

【数２８】Ｒ２＝ｆ（Ｋ’，ｒ１）

証明器が正しい証明補助情報ｔｐを保持している場合には、Ｋ’は証明情報Ｋに一致し、

【０２０３】

【数２９】Ｒ２＝ｆ（Ｋ，ｒ）

となる。

【０２０４】検証器２０はｆ（Ｋ，ｒ）を求めてＲ２と比較し、両者が等しい場合に限り、証明器３０が利用資格を有するものと判定する。

【０２０５】［第７の実施例］つぎに第７の実施例について説明する。この実施例は、認証対象の権利が複数あり、どの権利について認証するかを予め決めるようになっている。どの権利を認証するかは、権利の識別情報を入力したり、予め定められた規則で計算を行なって決定する。他の構成は第６の実施例と同様である。

【０２０６】この実施例の検証器２０は、第６の実施例（図５）の構成に加え、第１の秘密情報保持部２０６および第１の証明補助情報管理部２０７を設けている。また、証明器３０は、第２の秘密情報保持部３０６（図５の秘密情報保持部３０１）および第２の証明補助情報管理部３０７（図５の秘密情報保持部３０２）を有している。図６において、図５と対応する箇所には対応する符号を付した。

【０２０７】この実施例の証明補助情報発行器１０は、検証器１０および証明器２０の要求にそれぞれ応答して対応する証明補助情報を発行する。

【０２０８】利用資格の検証に先立ち、第２の通信部２０５から権利の識別情報を入力するか、事前に定められた規則にしたがって計算することにより、どの権利を検証するかを決定する。

【０２０９】検証器２０の第１の証明補助情報管理部２０７は、試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【０２１０】第１の試験情報計算部２０９は、第１の乱

数を生成し、少なくとも乱数と権利の識別情報とを併せて試験情報とする。この試験情報は、第２の通信部２０５から証明器３０の第３の通信部３０５へと伝達される。

【０２１１】証明器３０の第２の試験情報計算部３０９は、第２の乱数を生成して、これを第２の試験情報とする。第３の通信部３０５は、第２の試験情報を検証器２０の第２の通信部２０５に伝達する。

【０２１２】検証器２０の第２の一方向性関数計算部２０３は、秘密情報保持部２０６が保持する秘密情報と権利識別情報に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【０２１３】第１の応答情報計算部２１０は、一方向性関数の計算結果と証明補助情報とを演算し、証明情報を求める。第１の応答情報計算部２１０は、少なくとも第２の試験情報と検証器２０から証明器３０に伝達した情報とを第２の一方向性関数計算部に入力し、ここで得られた値と、伝達した情報そのものとように第１の応答情報を生成する。この第１の応答情報は、第２の通信部２０５から第３の通信部３０５へと伝達される。

【０２１４】証明器３０の第３の一方向性関数計算部３０４は、第２の秘密情報保持部２０６が保持する秘密情報と権利識別情報とに対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【０２１５】第２の証明補助情報管理部３０７は、試験情報に含まれる権利の識別情報に対応する証明補助情報を検索する。

【０２１６】第２の応答情報計算部３１０は、一方向性関数の計算結果と証明補助情報とを演算し、証明情報を求める。次いで、第１の応答情報が、第２の試験情報と証明情報とを含む情報に対し、第３の一方向性関数計算部を適用して得られる値と、第１の応答情報（その一部）とを照合する。値が所定の関係を満たさなければ意味のない値を生成して第２の応答情報とし、所定の関係を満たせば、後述の内部状態の変更と応答情報の計算を行う。

【０２１７】内部状態管理部３１２は、権利識別情報に対応する内部状態を検索し、第１の試験情報もしくは第１の応答情報で伝達された情報に応じて、内部状態を変更する。

【０２１８】第３の一方向性関数計算部３０４は、証明情報と、第１の試験情報に含まれる第１の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用し、第２の応答情報計算部３１０は、この値を第２の応答情報とする。第３の通信部３０５は、応答情報を第２の通信部２０５へ伝達する。

【０２１９】検証器２０の第２の一方向性関数計算部２０３は、証明情報と試験情報の乱数に対し、逆関数を求めることが少なくとも計算量的に困難な一方向性関数を適用する。

【０２２０】第１の応答情報検証器２１１は、一方向性関数の適用結果と、第２の応答情報とを比較し、一致する場合に限り利用資格があるものと判定する。

【０２２１】以下、第７の実施例の認証プロトコルについて説明する。

【０２２２】第７の実施例では、検証器の証明補助情報ｔｖと証明器の証明補助情報ｔｐを以下のように定める。

【０２２３】

【数３０】

ｔｖ＝Ｋ－ｆ（ｄｖ，ｎ）

ｔｐ＝Ｋ－ｆ（ｄｐ，ｎ）

ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器の秘密情報、ｄｐは証明器の秘密情報、ｎは検証すべき権利を識別する情報である。

【０２２４】検証器２０から証明器３０に送る第１の試験情報Ｃ１は、ｒ１を乱数として、

【０２２５】

【数３１】Ｃ１＝（ｎ，ｒ１）

である。

【０２２６】３０証明器は、第２の試験情報Ｃ２を検証器２０へ送る。

【０２２７】

【数３２】Ｃ２＝ｒ２

ここで、ｒ２は乱数である。

【０２２８】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いで、以下の計算により第１の応答情報Ｒ１を求める。

【０２２９】

【数３３】Ｒ１＝（ｍ，ｆ（Ｋ，ｒ２，ｍ））

ここで、ｍは検証器２０から証明器３０へと伝達する情報である。

【０２３０】証明器３０は、以下の計算によりＫ’を求める。

【０２３１】

【数３４】Ｋ’＝ｔｐ＋ｆ（ｄｐ，ｎ）

証明補助情報ｔｐが正しい場合には、Ｋ’は証明情報Ｋと一致する。

【０２３２】証明器３０はｆ（Ｋ’，ｒ２，ｍ）を計算して、Ｒ１の第２項と比較する。両者が等しい場合には、検証器２０から伝達された情報ｍにしたがい、検証すべき権利に対応する内部状態を変更する。たとえば、ｍが利用の都度課金される額であれば、プリペイドの額を相応分だけ減じる。

【０２３３】次いで、証明器３０は第２の応答情報Ｒ２を求める。

【０２３４】

【数３５】Ｒ２＝ｆ（Ｋ’，ｒ１）

証明器が正しい証明補助情報ｔｐを保持している場合には、Ｋ’は証明情報Ｋに一致し、

【０２３５】
【数３６】Ｒ２＝ｆ（Ｋ，ｒ）
となる。
【０２３６】検証器２０はｆ（Ｋ，ｒ）を求めてＲ２と比較し、両者が等しい場合に限り、証明器３０が利用資格を有するものと判定する。
［第８の実施例］つぎに第８の実施例について説明する。第８の実施例は、第７の実施例において利用制限情報を導入したものである。第８の実施例の構成は第７の実施例と同様に図６に示すように構成される。
【０２３７】以下、第８の実施例の認証プロトコルについて説明する。
【０２３８】第８の実施例では、検証器２０の証明補助情報ｔｖと証明器３０の証明補助情報ｔｐを以下のように定める。
【０２３９】
【数３７】
ｔｖ＝Ｋ－ｆ（ｄｖ，ｎ）
ｔｐ＝Ｋ－ｆ（ｄｐ，ｎ，Ｌ）
ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器２０の秘密情報、ｄｐは証明器３０の秘密情報、ｎは検証すべき権利を識別する情報、Ｌは使用制限記述である。
【０２４０】検証器２０から証明器３０に送る第１の試験情報Ｃ１は、ｒ１を乱数として、
【０２４１】
【数３８】Ｃ１＝（ｎ，ｒ１）
である。
【０２４２】証明器３０から検証器２０に送る第２の試験情報Ｃ２は、ｒ２を乱数として、
【０２４３】
【数３９】Ｃ２＝ｒ２
である。
【０２４４】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いで、以下の計算により第１の応答情報Ｒ１を求める。
【０２４５】
【数４０】Ｒ１＝（ｍ，ｆ（Ｋ，ｒ２，ｍ））
ここで、ｍは検証器２０から証明器３０へと伝達する情報である。
【０２４６】証明器３０は、以下の計算によりＫ’を求める。
【０２４７】
【数４１】Ｋ’＝ｔｐ＋ｆ（ｄｐ，ｎ）
証明補助情報ｔｐが正しい場合には、Ｋ’は証明情報Ｋと一致する。
【０２４８】証明器はｆ（Ｋ’，ｒ２，ｍ）を計算して、Ｒ１の第２項と比較する。両者が等しい場合には、検証器２０から伝達された情報ｍにしたがい、検証すべき権利に対応する内部状態を変更する。　次いで、証明器３０は第２の応答情報Ｒ２を求める。
【０２４９】
【数４２】Ｒ２＝（Ｌ，ｆ（ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ），ｒ，Ｌ））
証明器３０が正しい証明補助情報ｔｐを保持している場合には、Ｋ’は証明情報Ｋに一致し、
【０２５０】
【数４３】Ｒ２＝（Ｌ，ｆ（Ｋ，ｒ，Ｌ））
となる。
【０２５１】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いでｆ（Ｋ，ｒ）を求めてＲ２の第２項と比較し、両者が等く、かつ使用制限記述Ｌが使用条件を満たす場合に限り、証明器３０が利用資格を有するものと判定する。
【０２５２】ここでは使用制限記述Ｌが使用条件を満たすか否かの判定を検証器２０で行うものとしたが、証明器３０で行うようにしてもよい。
【０２５３】［第９の実施例］第９の実施例は、第８の実施例において検証器２０に復号部２０８を設けたものである。図７は第９の実施例の構成を示しており、この図において図６と対応する箇所には対応する符号を付した。
【０２５４】第９の実施例では、扱う情報および検証手順は第８の実施例と同じである。証明器が利用資格を有すると判定した場合には、復号部２０８が、証明情報Ｋあるいはこれを用いて計算可能な値を鍵として用い、暗号化された情報を復号する。
【０２５５】［第１０の実施例］つぎに第１０の実施例について説明する。この実施例は利用履歴を管理できるようにしたものである。
【０２５６】図８は、第１０の実施例の構成を示しており、この図において、図７と対応する箇所には対応する符号を付した。図８においては、証明器３０に履歴管理部３０８を設けている。
【０２５７】以下、第１０の実施例の認証プロトコルについて説明する。
【０２５８】この認証手順は図１０にも示す。第５～第９の実施例の各動作は第１０の実施例に含まれているので第５～第９の実施例の動作も図１０から理解できる。
【０２５９】第１０の実施例では、検証器の証明補助情報ｔｖと証明器の証明補助情報ｔｐを以下のように定める。
【０２６０】
【数４４】
ｔｖ＝Ｋ－ｆ（ｄｖ，ｎ）
ｔｐ＝Ｋ－ｆ（ｄｐ，ｎ，Ｌ）
ここで、Ｋは証明情報、ｆは一方向性関数、ｄｖは検証器２０の秘密情報、ｄｐは証明器３０の秘密情報、ｎは検証すべき権利を識別する情報、Ｌは使用制限記述である。使用制限記述Ｌは、たとえば使用期限を表すビット

列である。

【０２６１】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。

【０２６２】検証器２０から証明器３０に送る第１の試験情報Ｃ１は、ｒ１を乱数として、

【０２６３】

【数４５】Ｃ１＝（ｎ，Ｉ，ｒ，ｓ）

である。ここで、Ｉは検証器から証明器に伝送する情報、ｓは

【０２６４】

【数４６】ｓ＝ｆ（Ｋ，Ｉ，ｒ）

なる値である。

【０２６５】証明器３０は、以下の計算によりＫ’を求める。

【０２６６】

【数４７】Ｋ’＝ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ）

次いで証明器３０は、ｆ（Ｋ’，Ｉ，ｒ）を計算し、ｓと比較する。ｓが一致した場合に限り、Ｉを含む情報を履歴保持部３０８に格納する。

【０２６７】証明器３０は、第２の試験情報Ｃ２を検証器に送る。

【０２６８】

【数４８】Ｃ２＝ｒ２

ここで、ｒ２は乱数である。

【０２６９】検証器２０は、ｔｖ＋ｆ（ｄｖ，ｎ）を計算しＫを求める。次いで、以下の計算により第１の応答情報Ｒ１を求める。

【数４９】Ｒ１＝（ｍ，ｆ（Ｋ，ｒ２，ｍ））

ここで、ｍは検証器から証明器へと伝達する情報である。証明器は、以下の計算によりＫ’を求める。

【０２７０】

【数５０】Ｋ’＝ｔｐ＋ｆ（ｄｐ，ｎ）

証明補助情報ｔｐが正しい場合には、Ｋ’は証明情報Ｋと一致する。

【０２７１】証明器３０はｆ（Ｋ’，ｒ２，ｍ）を計算して、Ｒ１の第２項と比較する。両者が等しい場合には、検証器２０から伝達された情報ｍにしたがい、検証すべき権利に対応する内部状態を変更する。

【０２７２】次いで、証明器３０は第２の応答情報Ｒ２を求める。

【０２７３】

【数５１】Ｒ２＝（Ｌ，ｆ（ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ），ｒ，Ｌ））

証明器３０が、正しい証明補助情報ｔｐを保持している場合には、

【０２７４】

【数５２】ｔｐ＋ｆ（ｄｐ，ｎ，Ｌ）＝Ｋ－ｆ（ｄｐ，ｎ，Ｌ）＋ｆ（ｄｐ，ｎ，Ｌ）＝Ｋ

となって、証明情報Ｋを復元でき、

【０２７５】

【数５３】Ｒ２＝（Ｌ，ｆ（Ｋ，ｒ，Ｌ））

となる。

【０２７６】検証器２０は、ｆ（Ｋ，ｒ）を求めてＲ２と比較する。両者が等く、かつＬが使用条件を満たす場合に限り、証明器３０が利用資格を有するものと判定する。

【０２７７】ここでは、使用制限記述Ｌが使用条件を満たすか否かの判定を検証器２０で行うものとしたが、証明器３０で行うようにしてもよい。

【０２７８】以上の実施例では、一方向性関数としてＭＤ５やＳＨＡを例として挙げたが、代わりにＤＥＳなどの慣用暗号系を用いてもよい。

【０２７９】以上の本実施例では、検証器の認証と、証明器が権利を有することの証明に使う情報を同一の証明情報としたが、それぞれについて別個の証明情報を用いることとし、証明情報保持部、秘密情報保持部、証明補助情報管理部で適切な情報を扱うようにしてもよい。

【０２８０】以上の実施例では、耐タンパー性のあるハードウェアを用いることはとくに前提にしていないが、証明情報保持部、秘密情報保持部、および一方向性関数計算部を耐タンパー性のあるハードウェアで保護することにより、不正の危険を低減することができる。

【０２８１】以上の実施例では、ソフトウェアの実行の可否の制御のために本発明の利用資格検証装置を用いたが、証明補助情報を、実世界で提供されている種々のサービスで通常用いられているチケット（切符）として用いることが可能である。

【０２８２】以上の実施例では、証明補助情報として、一方向性関数用いて得た値を証明情報から減じた結果を用いたが、ビット毎の排他的論理和など、逆算が可能な演算の組み合わせを証明情報に適用した結果であればよい。

【０２８３】［適用例］つぎに、実施例の具体的な適用例について説明する。なお、以下では、証明補助情報のことをチケットと呼ぶ。

【０２８４】まず、ソフトウエアのアクセス制御に用いる場合について説明する。

【０２８５】図１６は、ソフトウェアのアクセス制御をネットワーク上で行う例を示している。なお、図１６において図１と対応する箇所には対応する符号を付した。図１６において、利用者計算機１０００とチケット発行計算機２０００とがネットワーク３０００で接続されている。ネットワーク３０００はＷＡＮでもＬＡＮでもよい。利用者計算機１０００はハードウェア１００１に所定のオペレーティングシステム１００２がインストールされ、このオペレーティングシステム１００２上でアプリケーションプログラム１００３および証明プログラム３０が動作する。アプリケーションプログラム１００３には検証プログラム２０が埋め込まれている。アプリケーションプログラム１００３は記録媒体の形態で提供さ

れてもよいし、オンラインで提供されていもよい。証明プログラム３０の一部は利用者計算機１０００に実装された耐タンパー装置上で実行されることが好ましい。

【０２８６】チケット発行計算機２０００もハードウェア２００１およびオペレーティングシステム２００２を有し、チケット発行サーバ３０が動作するようになっている。

【０２８７】ユーザは、アプリケーション１００３を利用したい場合には、証明用補助情報（チケット）の発行をチケット発行サーバに要求する。この要求は、ユーザの識別番号とアプリケーションの識別番号とを伴う。チケット発行サーバ１０は、ユーザの識別番号およびアプリケーションの識別番号に基づいてそれぞれユーザの秘密情報および公開鍵の法数および証明情報を取り出す。そして証明補助情報を計算して利用計算機１０００の証明プログラム２０に渡す。

【０２８８】以降、証明プログラム３０と検証プログラム２０とが試験情報Ｃおよび応答情報Ｒをやり取りして認証を行い、認証が成功したならばアプリケーションプログラムが利用可能になる。

【０２８９】ソフトウェア（アプリケーション１００３）の保護の手法としてはソフトウェアの少なくとも一部を暗号鍵で暗号しておくことが考えられる。ソフトウェアの暗号鍵をＫとし、乱数をｒとする。安全のためには、鍵Ｋそのものがソフトウェアに含まれないことが望ましい。鍵Ｋそのものはソフトウェアに含まれない場合、暗号化されたソフトウェアの一部を復号し、所定の条件を満たすかどうか検査すればよい。

【０２９０】つぎに実施例を改札装置の制御に用いる例を説明する。図１７は本実施例が適用された改札システムを示しており、この図において、ＩＣカード４０００には証明器３０を実現するプログラムがインストールされている。チケット発行端末５０００はＩＣカードが着脱可能なものであり、チケット発行サーバ３０と通信してＩＣカード４０００に証明補助情報（チケット）を書き込む。ユーザは入場するときにＩＣカード４０００を入場ゲート６０００に提示し（例えばスロットに挿入して）、この間、入場ゲート６０００の検証装置１０とＩＣカード４０００の証明装置２０とが相互に通信して認証を行う。認証が成功すればユーザは入場ゲート６０００を通過することが可能になる。

【０２９１】

【発明の効果】一般に公開鍵暗号系と比較して、ハッシュは数千倍高速である。ＢｒｕｃｅＳｃｈｎｅｉｅｒ．Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ（ＳｅｃｏｎｄＥｄｉｔｉｏｎ），Ｗｉｌｅｙ，１９９６によれば、１２８ビットのダイジェストを計算するＭＤ５アルゴリズムを米国インテル社製のプロセッサ（３３ＭＨｚの４８６ＳＸ、商標）で実行したとき、毎秒１７４ＭＢ符号化できる。前述のように、同書によれば、法数１０２４ビット・公開鍵８ビットのＲＳＡ暗号系をＳＰＡＲＣ２で実行する時間は、署名が０．９７秒、検証が０．０８秒かかっている。したがって、認証機構を公開鍵暗号系からハッシュに変更することにより、計算量を数千分の１に削減し、実行速度を向上させることが可能である。

【０２９２】以上のように、本発明の利用資格検証装置によれば、ソフトウェアのアクセス制御を効率よく実行できる。さらに、検証器側に証明補助情報を使用することにより、アーケードゲームや各種サービスを実行できるハードウェアを制限でき、ハードに対するライセンス料の徴収やフランチャイズ制を実現可能である。

【図面の簡単な説明】

【図１】　この発明の第１の実施例の構成を示すブロック図である。

【図２】　この発明の第２の実施例および第３の実施例の構成を示すブロック図である。

【図３】　この発明の第４の実施例の構成を示すブロック図である。

【図４】　この発明の第５の実施例の構成を示すブロック図である。

【図５】　この発明の第６の実施例の構成を示すブロック図である。

【図６】　この発明の第７の実施例および第８の実施例の構成を示すブロック図である。

【図７】　この発明の第９の実施例の構成を示すブロック図である。

【図８】　この発明の第１０の実施例の構成を示すブロック図である。

【図９】　この発明の第５の実施例の全体の動作を説明する図である。

【図１０】　この発明の第１０の実施例の全体の動作を説明する図である。

【図１１】　この発明の第１の実施例の証明補助情報発行器の動作を説明するフローチャートである。

【図１２】　この発明の第１の実施例の検証器の動作を説明するフローチャートである。

【図１３】　この発明の第１の実施例の証明器の動作を説明するフローチャートである。

【図１４】　この発明の第６の実施例の検証器の動作を説明するフローチャートである。

【図１５】　この発明の第１の実施例の証明器の動作を説明するフローチャートである。

【図１６】　この発明の実施例の第１の適用例を示すブロック図である。

【図１７】　この発明の実施例の第２の適用例を示すブロック図である。

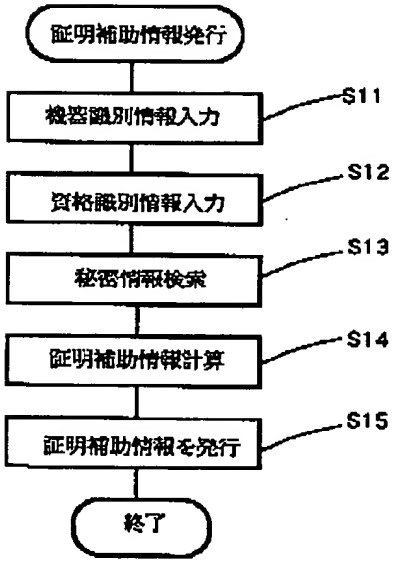
【符号の説明】

１０　　証明補助情報発行器

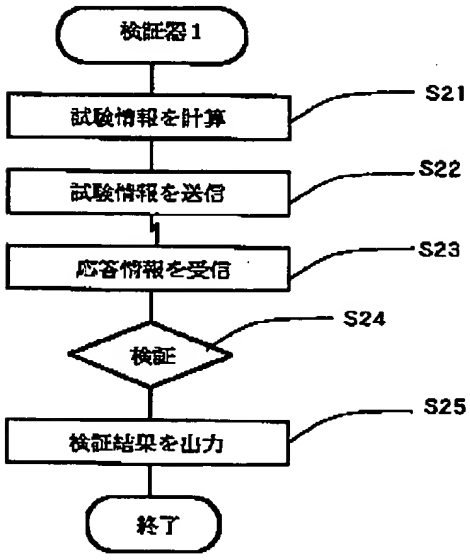
２０　　検証器

３０　証明器
１０１　第１の通信部
１０２　秘密情報管理部
１０３　証明情報管理部
１０４　第１の一方向性計算部
１０５　証明補助情報計算部
２０１　証明情報保持部
２０２　試験情報計算部
２０３　第２の一方向性関数計算部
２０４　応答情報検証器
２０５　第２の通信部
２０６　第１の秘密情報保持部
２０７　第１の証明補助情報管理部
２０８　復号部
２０９　第１の試験情報計算部
２１０　第１の応答情報計算部
２１１　第１の応答情報検証部
３０１　秘密情報保持部
３０２　証明補助情報管理部
３０３　応答情報計算部
３０４　第３の一方向性関数計算部
３０５　第３の通信部
３０６　第２の秘密情報保持部
３０７　第２の証明補助情報管理部
３０８　履歴管理部
３０９　第２の試験情報計算部
３１０　第２の応答情報計算部
３１１　第２の応答情報検証部
３１２　内部状態管理部

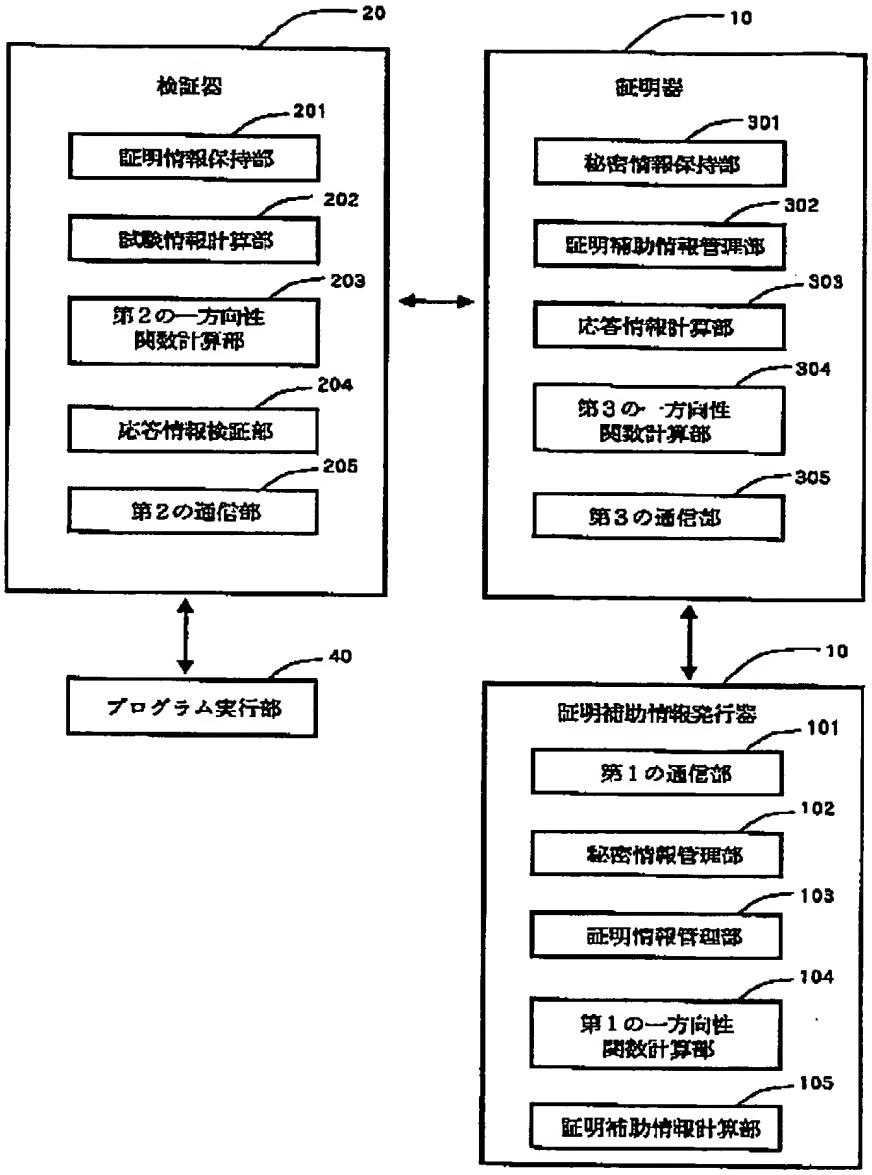
【図１１】



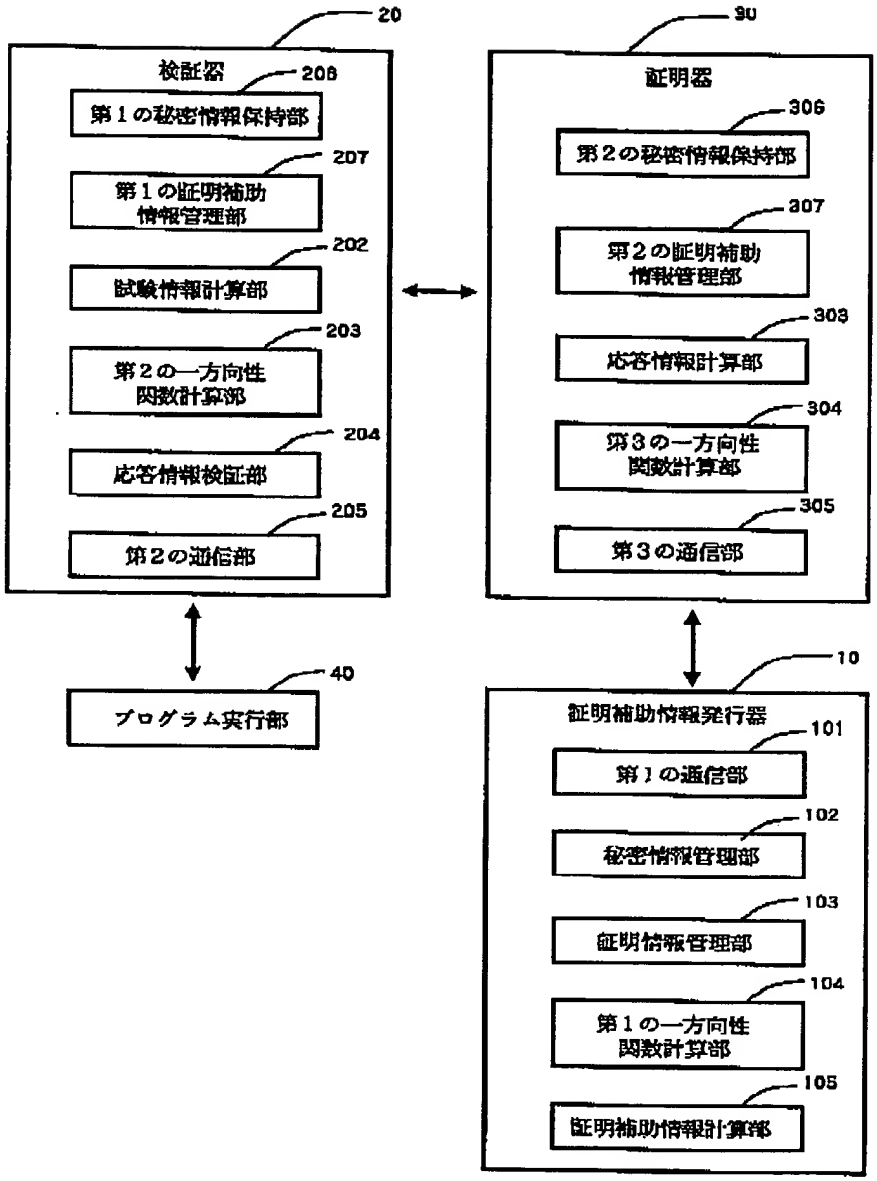
【図１２】



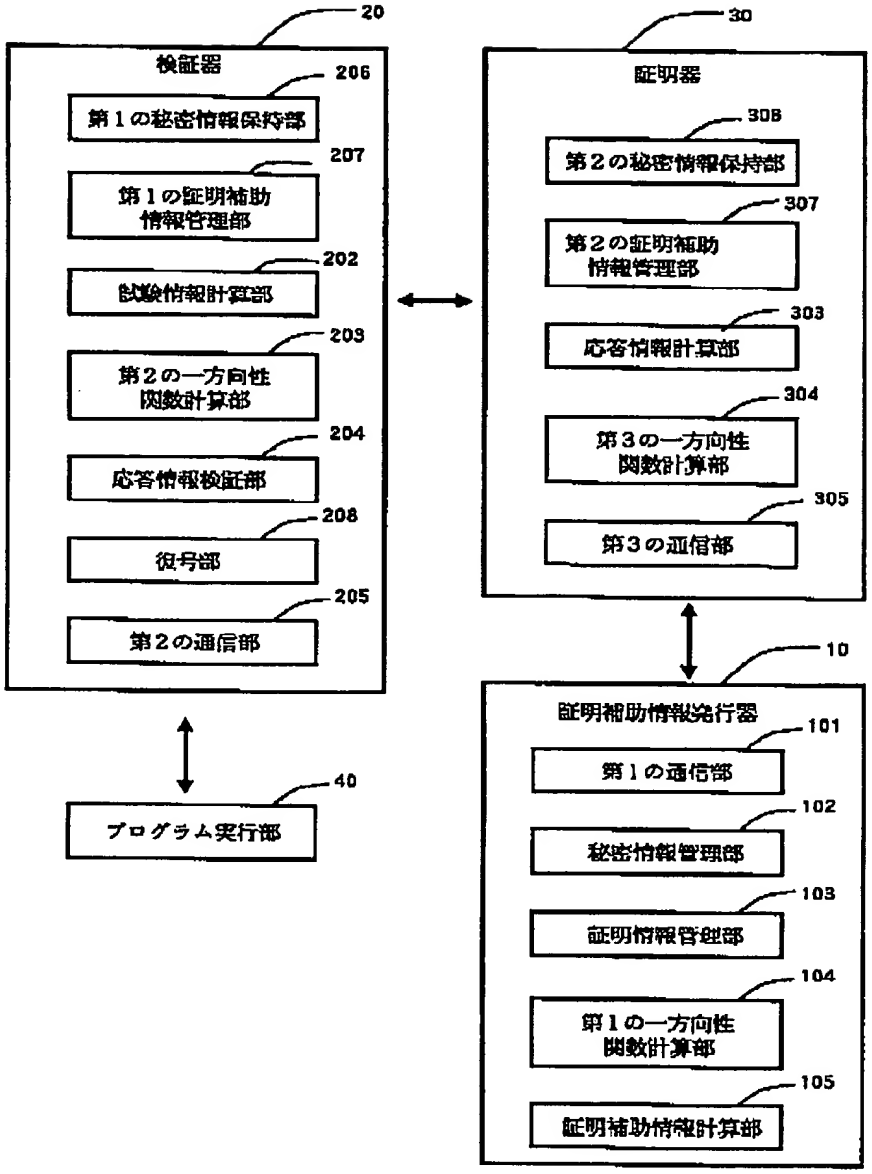
【図１】


20
検証器
201
証明情報保持部
202
試験情報計算部
203
第２の一方向性関数計算部
204
応答情報検証部
205
第２の通信部
40
プログラム実行部
10
証明器
301
秘密情報保持部
302
証明補助情報管理部
303
応答情報計算部
304
第３の一方向性関数計算部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

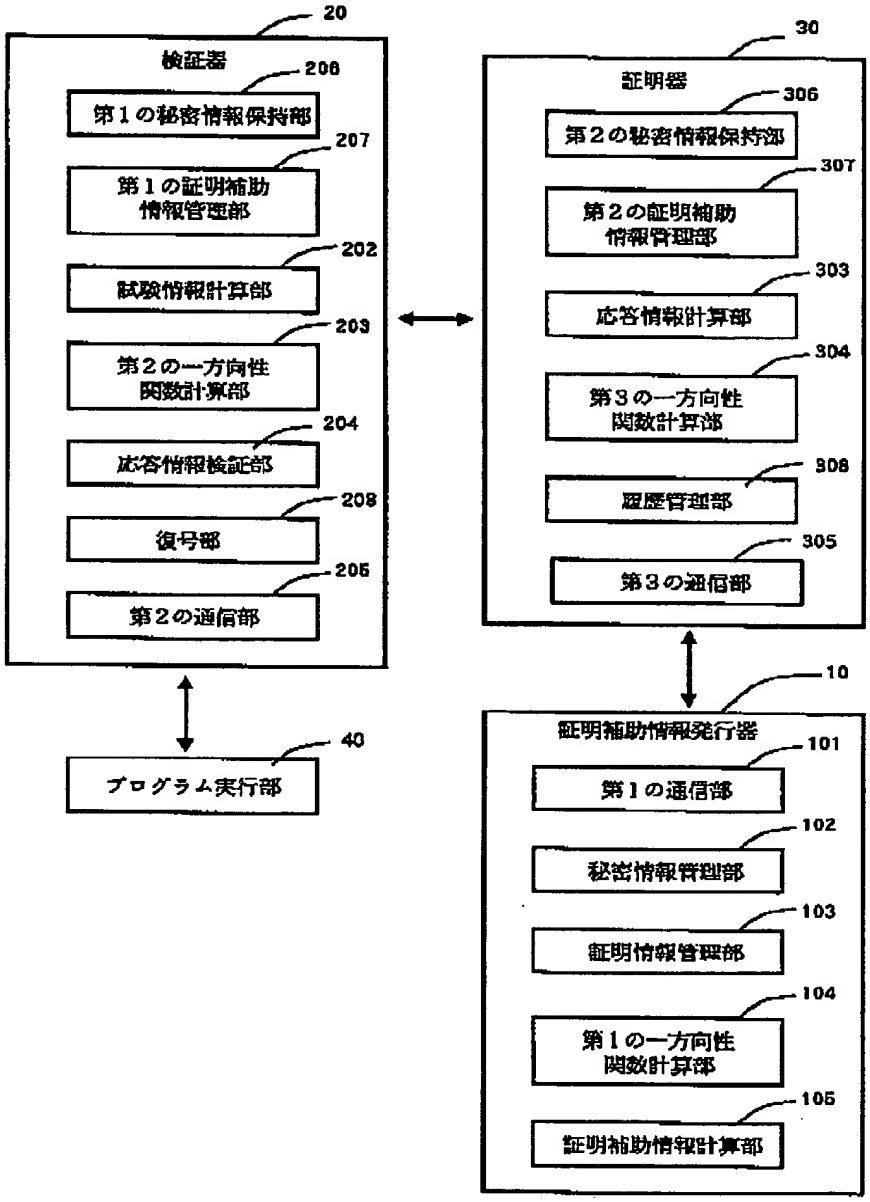
【図２】


20
検証器
208
第１の秘密情報保持部
207
第１の証明補助情報管理部
202
試験情報計算部
203
第２の一方向性関数計算部
204
応答情報検証部
205
第２の通信部
40
プログラム実行部
90
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
303
応答情報計算部
304
第３の一方向性関数計算部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

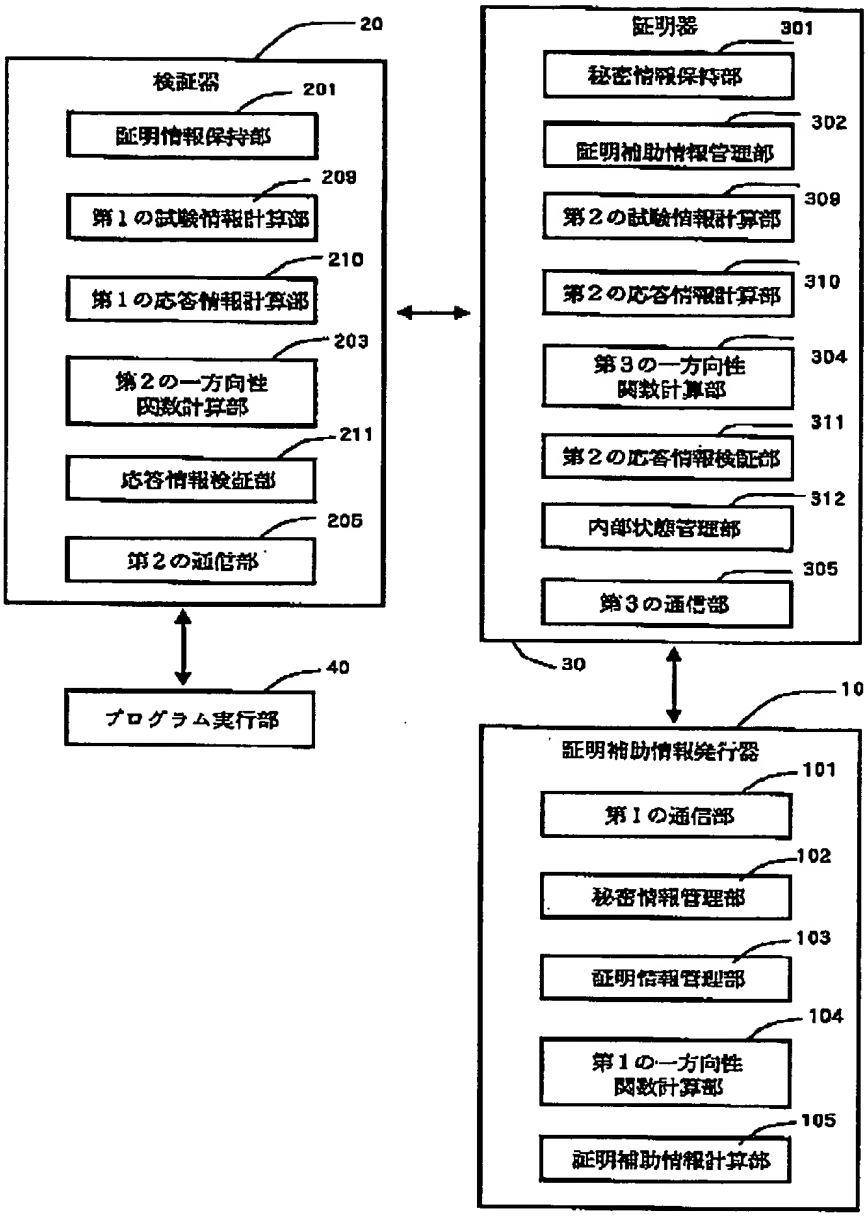
【図３】


20
検証器
206
第１の秘密情報保持部
207
第１の証明補助情報管理部
202
試験情報計算部
203
第２の一方向性関数計算部
204
応答情報検証部
208
復号部
205
第２の通信部
40
プログラム実行部
30
証明器
308
第２の秘密情報保持部
307
第２の証明補助情報管理部
303
応答情報計算部
304
第３の一方向性関数計算部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

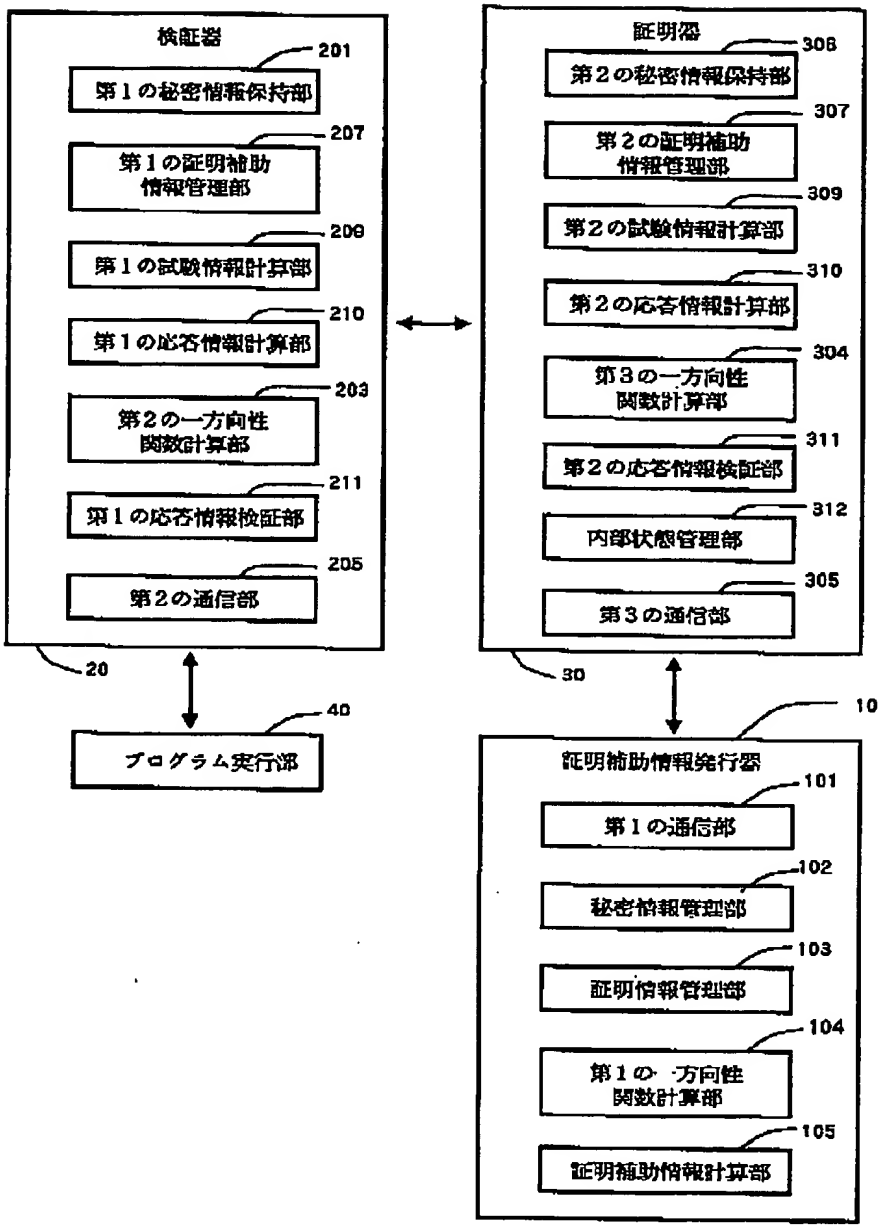
【図４】


20
検証器
206
第１の秘密情報保持部
207
第１の証明補助情報管理部
202
試験情報計算部
203
第２の一方向性関数計算部
204
応答情報検証部
208
復号部
205
第２の通信部
40
プログラム実行部
30
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
303
応答情報計算部
304
第３の一方向性関数計算部
308
履歴管理部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

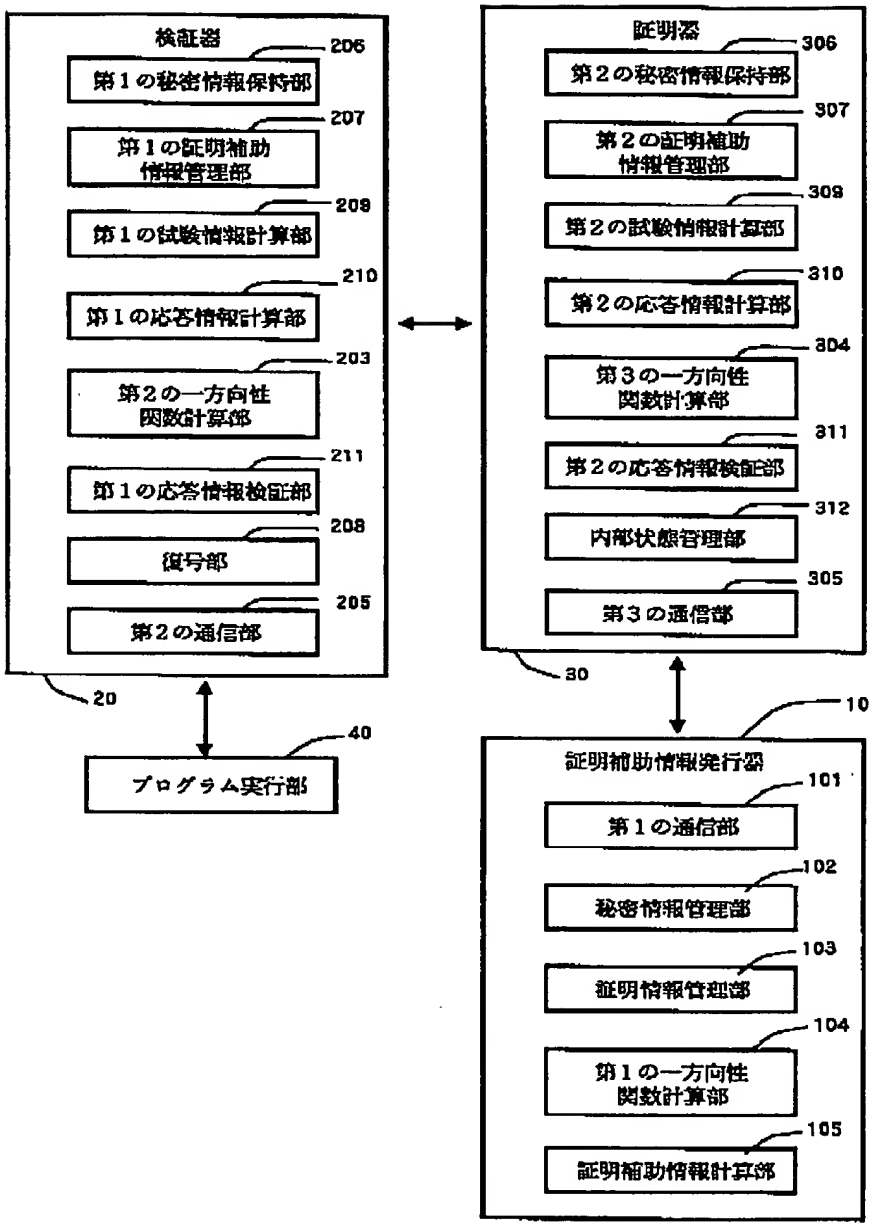
【図５】


検証器
20
証明情報保持部
201
第１の試験情報計算部
209
第１の応答情報計算部
210
第２の一方向性関数計算部
203
応答情報検証部
211
第２の通信部
205
プログラム実行部
40
証明器
301
秘密情報保持部
302
証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

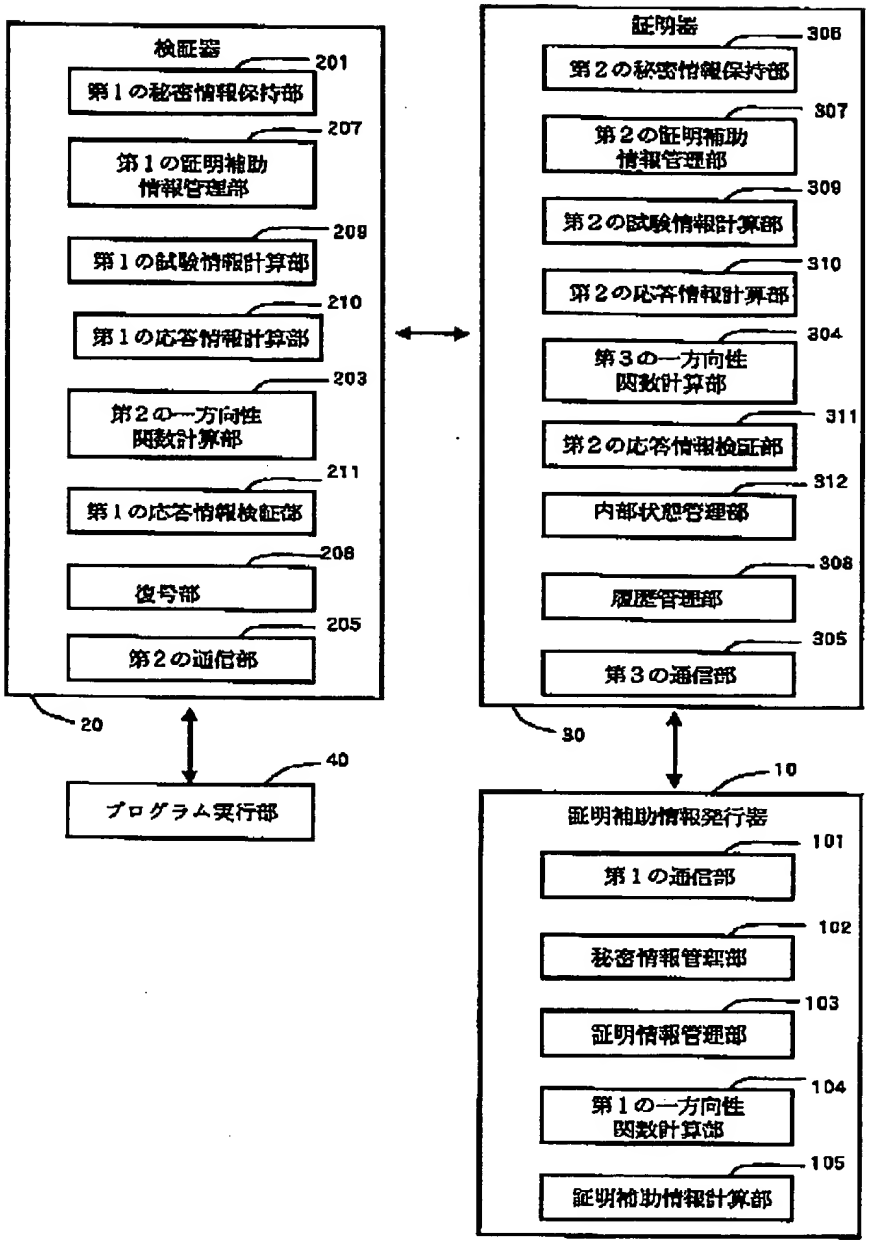
【図６】


検証器
201
第１の秘密情報保持部
207
第１の証明補助情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
第１の応答情報検証部
205
第２の通信部
20
40
プログラム実行部
証明器
308
第２の秘密情報保持部
307
第２の証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

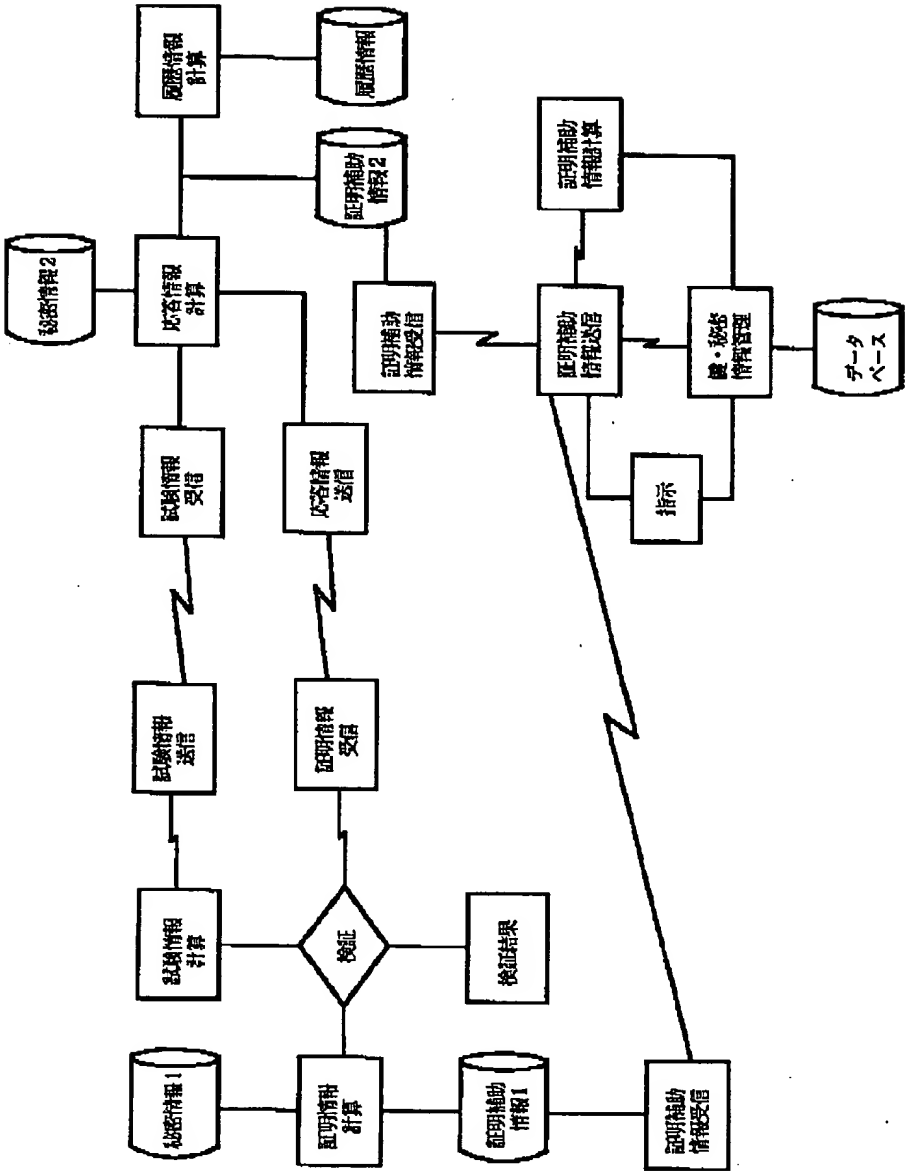
【図７】


検証器
206
第１の秘密情報保持部
207
第１の証明補助情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
第１の応答情報検証部
208
復号部
205
第２の通信部
20
40
プログラム実行部
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

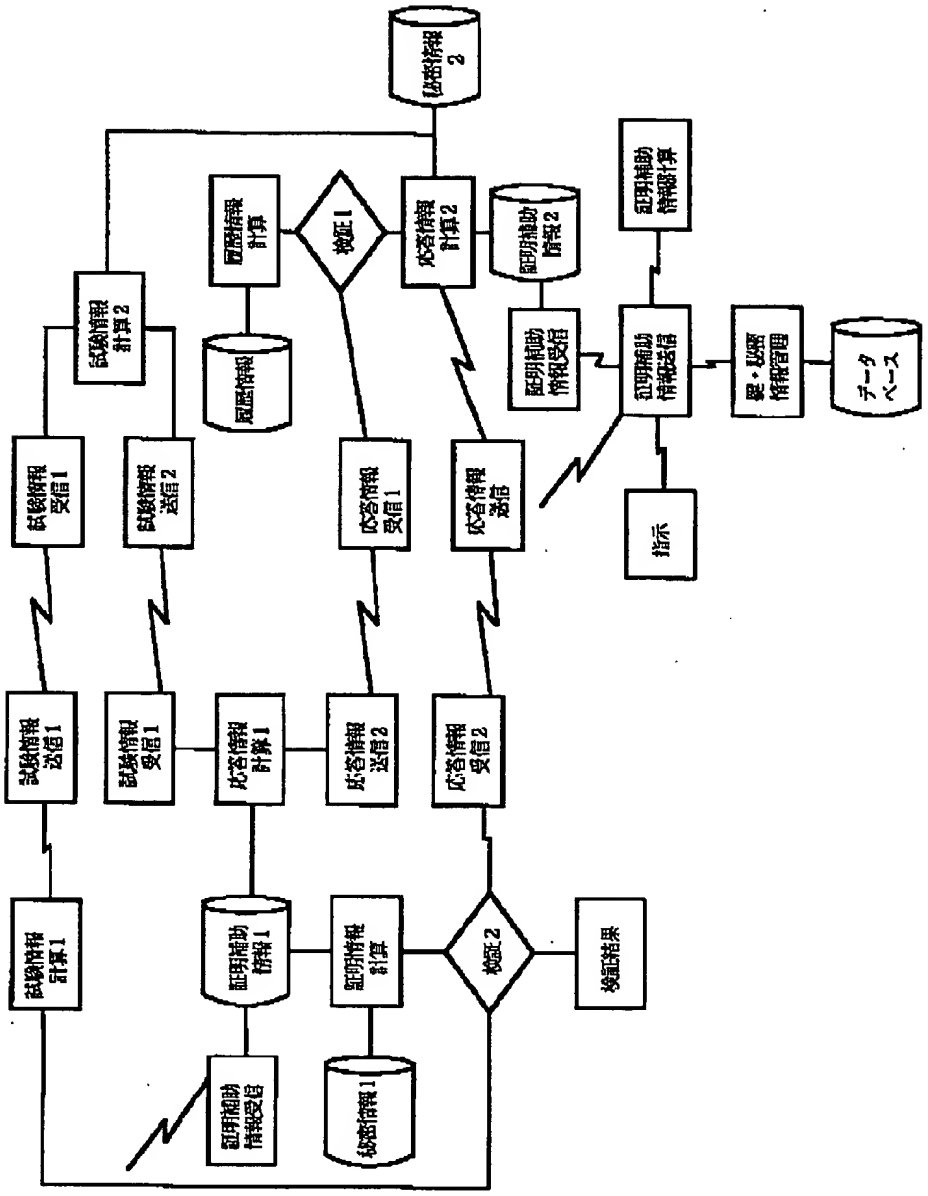
【図８】


検証器
201
第１の秘密情報保持部
207
第１の証明補助情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
第１の応答情報検証部
208
復号部
205
第２の通信部
20
40
プログラム実行部
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
308
履歴管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

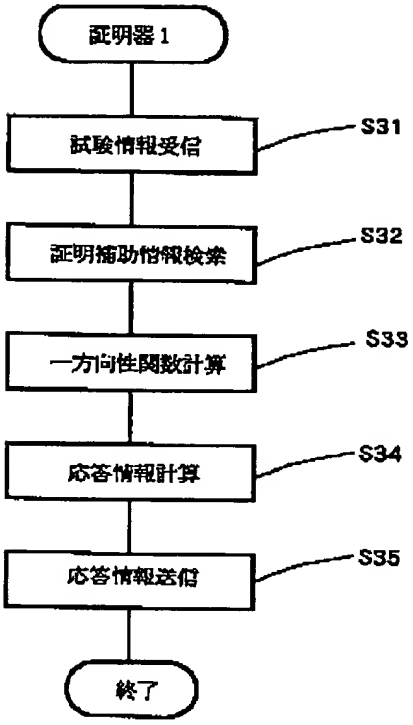
【図９】


履歴情報計算
履歴情報
証明補助情報2
秘密情報2
応答情報計算
証明補助情報計算
証明補助情報受信
証明補助情報送信
鍵・秘密情報管理
データベース
試験情報受信
応答情報送信
指示
試験情報送信
証明情報受信
試験情報計算
検証
検証結果
秘密情報1
証明情報計算
証明補助情報1
証明補助情報受信

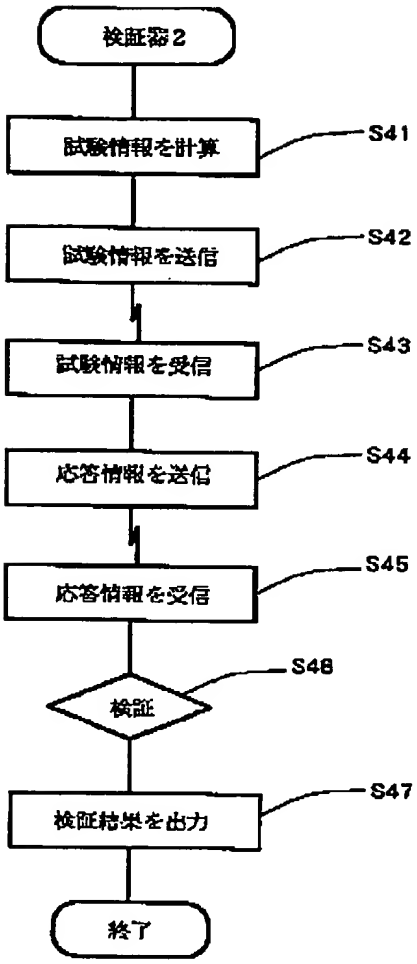
【図１０】


秘密情報2
履歴情報計算
検証1
応答情報計算2
証明補助情報2
証明補助情報計算
試験情報計算2
履歴情報
証明補助情報受信
証明補助情報送信
鍵・秘密情報管理
データベース
試験情報受信1
試験情報送信2
応答情報受信1
応答情報送信
指示
試験情報送信1
試験情報受信1
応答情報計算1
応答情報送信2
応答情報受信2
試験情報計算1
証明補助情報1
証明情報計算
検証2
検証結果
証明補助情報受信
秘密情報1

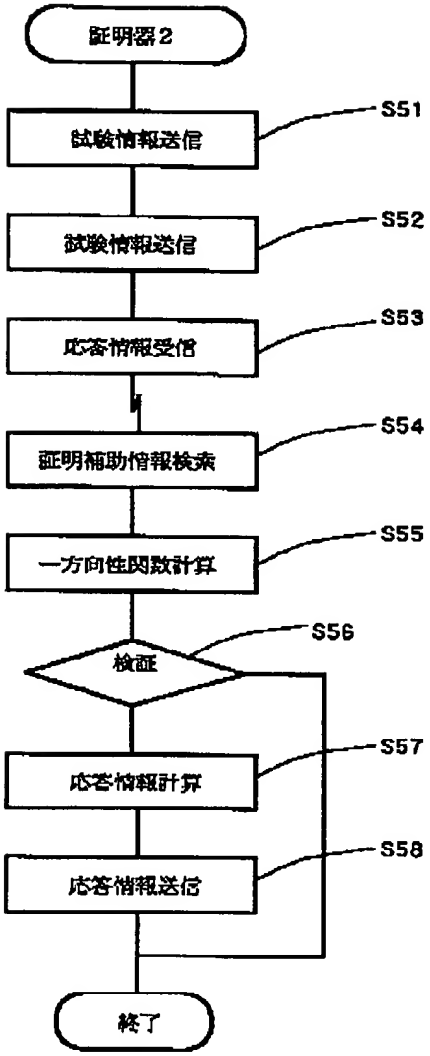
【図１３】


証明器1
試験情報受信
S31
証明補助情報検索
S32
一方向性関数計算
S33
応答情報計算
S34
応答情報送信
S35
終了

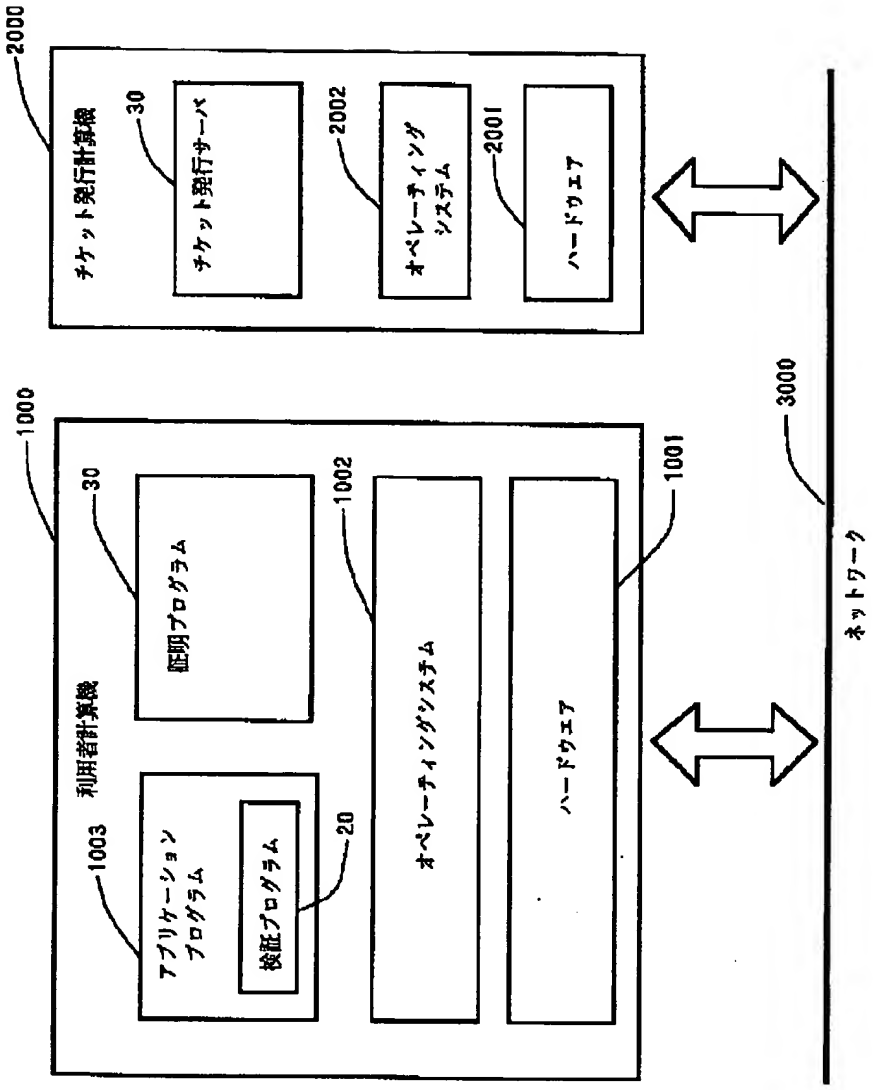
【図１４】


検証器2
試験情報を計算
S41
試験情報を送信
S42
試験情報を受信
S43
応答情報を送信
S44
応答情報を受信
S45
検証
S48
検証結果を出力
S47
終了

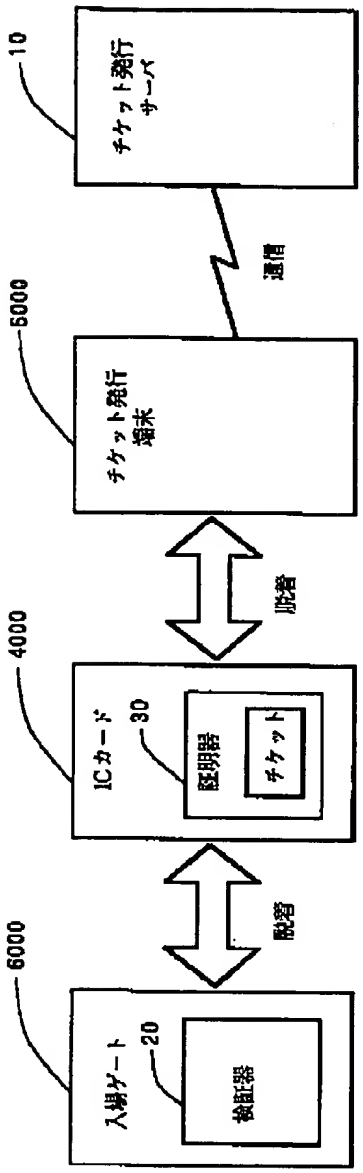
【図１５】


証明器2
S51
試験情報送信
S52
試験情報送信
S53
応答情報受信
S54
証明補助情報検索
S55
一方向性関数計算
S56
検証
S57
応答情報計算
S58
応答情報送信
終了

【図１６】


2000
チケット発行計算機
30
チケット発行サーバ
2002
オペレーティング システム
2001
ハードウエア
3000
ネットワーク
1000
利用者計算機
30
証明プログラム
1002
オペレーティングシステム
1001
ハードウエア
1003
アプリケーション プログラム
20
検証プログラム

【図１７】



フロントページの続き

(51) Int. Cl.[6]	識別記号	FI	
G09C 1/00	660	G06K 19/00	R

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-234262
(43)Date of publication of application : 27.08.1999

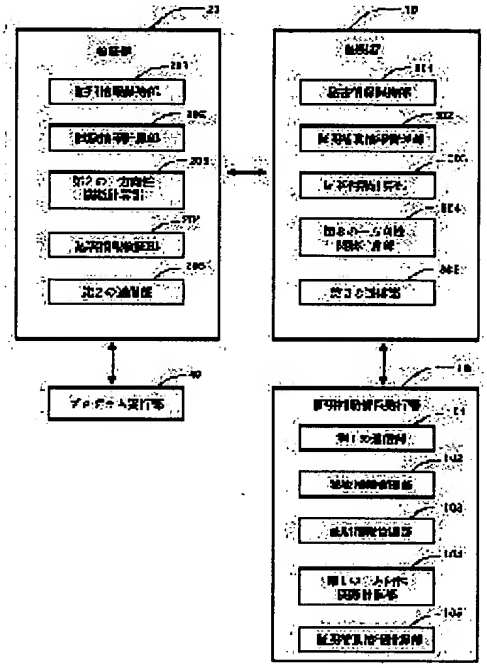
(51)Int.CI. H04L 9/32
G06F 9/06
G06K 19/10
G09C 1/00
G09C 1/00

(21)Application number : 10-027326
(22)Date of filing : 09.02.1998

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : NAKATSUYAMA HISASHI

(54) UTILIZATION QUALIFICATION VERIFYING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To perform high-speed authentication through a device of a small CPU power memory.
SOLUTION: A test information calculating part 202 of a verifier 20 generates a random number, and transmits both the random number and information on the identification of right to a testifier 10 as test information. A third unidirectional function calculating part 304 of the testifier 10 applies a unidirectional function to the right identification information of secret information and test information held by a secret information holding part 301. A response information calculating part 303 finds evidence information by operating the calculated result of the unidirectional function and evidence support information. Further, the third unidirectional function calculating part 304 applies a unidirectional function to the evidence information and the random number contained in the test information and returns them to the verifier 20 as response information. A second unidirectional function calculating part 203 of the verifier 20 applies a unidirectional function to the evidence information and the random number in the test information. A response information verifier 204 compares the applied result of the unidirectional function with the response information, and only when they are coincident, qualification to utilization is confirmed.



LEGAL STATUS

[Date of request for examination] 17.10.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section said certification auxiliary information issue section A certification information management means to manage the certification information used in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information. Said verification section A certification information maintenance means to hold certification information, and a trial information count means to calculate trial information, On the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] The certification information which said certification information maintenance means holds, and a response indication verification means to inspect whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Said certification section A confidential information maintenance means to hold secret information, and a certification auxiliary information management means to manage the certification auxiliary information that it uses for count of a response indication, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of trial information, and the confidential information which said confidential information maintenance means holds, To the value acquired based on the certification auxiliary information which said certification auxiliary information management means manages, said 3rd response indication count means to calculate a response indication by on the other hand making a tropism function count means act, Use rating verification equipment characterized by having the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 2] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section said certification auxiliary information issue section A certification information management means to manage the certification information used in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, It has the 1st means of

communications which transmits and receives information in process of count of certification auxiliary information. Said verification section The 1st confidential information maintenance means holding secret information, and the 1st certification auxiliary information management means which manages certification auxiliary information, On the other hand, the 2nd to which a trial information count means to calculate trial information, and asking for an inverse function apply a directivity function difficult in computational complexity at least A tropism function count means, The confidential information which said 1st confidential information maintenance means holds, and a response indication verification means to inspect whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Said certification section The 2nd confidential information maintenance means holding secret information, and the 2nd certification auxiliary information management means which manages the certification auxiliary information that it uses for count of a response indication, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of trial information, and the confidential information which said 2nd confidential information maintenance means holds, To the value acquired based on the certification auxiliary information which said 2nd certification auxiliary information management means manages, said 3rd response indication count means to calculate a response indication by on the other hand making a tropism function count means act, Use rating verification equipment characterized by having the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.

[Claim 3] It is use rating verification equipment carry out containing use limit description in count of the response indication generate at the certification auxiliary information are use rating verification equipment of claim 1 thru/or claim 2, combine with certification information and said certification information-management means manages the use limit description which is the information which shows use conditions, and combine with certification auxiliary information, and said certification auxiliary information-management means manages use limit description, and use at said certification section, and said certification section as the description.

[Claim 4] Use rating verification equipment characterized by decoding information, using the value acquired from certification information or certification information as a decode key of said decode means when it judges with it being use rating verification equipment of claim 1 thru/or claim 3, and having a decode means, and there being use rating.

[Claim 5] It is use rating verification equipment have the hysteresis management tool which is use rating verification equipment of claim 1 thru/or claim 4, and manages the hysteresis at the time of use rating verification, and combine with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information-management means manage transfer information, and carry out that trial information stores said transfer information to a hysteresis management tool at the time of use rating verification including transfer information further as the description.

[Claim 6] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section said certification auxiliary information issue section A certification information management means to manage the certification information used in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information. Said verification section A certification information maintenance means to hold certification information, and the 1st trial information count means which calculates the 1st trial information, On the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] To the 2nd trial information which

received, said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and calculates the 1st response indication, The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Said certification section A confidential information maintenance means to hold secret information, and a certification auxiliary information management means to manage the certification auxiliary information that it uses for count of a response indication, The internal-state management tool which manages the internal state corresponding to certification auxiliary information, and the 2nd trial information count means which calculates trial information, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of the received information, and the confidential information which said confidential information maintenance means holds, To the value acquired based on the certification auxiliary information which said certification auxiliary information management means manages, said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act, The 2nd trial information count means which calculates the 2nd trial information, and part or all of the 1st response indication and the 2nd trial information, To the value acquired based on the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages Use rating verification equipment characterized by having the 3rd [said] result on which the tropism function count means was made to act on the other hand, whether a response indication is equal and the 2nd response indication verification means to inspect, and the 3rd means of communications which transmit and receive information in process of the process of authentication of use rating, and certification auxiliary information count.

[Claim 7] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section said certification auxiliary information issue section A certification information management means to manage the certification information used in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information. Said verification section The 1st confidential information maintenance means holding secret information, and the 1st certification auxiliary information management means which manages certification auxiliary information, On the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the 1st trial information count means which calculates the 1st trial information, and asking for an inverse function] To the 2nd trial information which received, said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and calculates the 1st response indication, The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Said certification section The 2nd confidential information maintenance means holding secret information, and the 2nd certification auxiliary information management means which manages the certification auxiliary information that it uses for creation of a response indication, The internal-state management tool which manages the internal state corresponding to certification auxiliary information, and the 2nd trial information count means which calculates trial information, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of the received information, and the confidential

information which said confidential information maintenance means holds, To the value acquired based on the certification auxiliary information which said certification auxiliary information management means manages, said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act, The 2nd trial information count means which calculates the 2nd trial information, and part or all of the 1st response indication and the 2nd trial information, To the value acquired based on the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages Use rating verification equipment by which it is characterized [which has the 3rd / said / result on which the tropism function count means was made to act on the other hand, whether a response indication is equal and the 2nd response indication verification means to inspect, and the 3rd means of communications which transmit and receive information in process of the process of authentication of use rating, and certification auxiliary information count].

[Claim 8] It is use rating verification equipment carry out containing use limit description in count of the response indication generated in the certification auxiliary information are use rating verification equipment of claim 6 thru/or claim 7, combine with certification information and a certification information-management means manages the use limit description which is the information which shows use conditions, and combine with certification auxiliary information, manage a certification auxiliary information-management means and use limit description, and use at the certification section, and the certification section as the description.

[Claim 9] Use rating verification equipment characterized by decoding information, using the value acquired from certification information or certification information as a decode key of said decode means when it judges with it being use rating verification equipment of claim 6 thru/or claim 8, and having a decode means, and there being use rating.

[Claim 10] It is use rating verification equipment have the hysteresis management tool which is use rating verification equipment of claim 6 thru/or claim 9, and manages the hysteresis at the time of use rating verification, and combine with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information-management means manage transfer information, and carry out that trial information stores said transfer information to a hysteresis management tool at the time of use rating verification including transfer information further as the description.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the use rating verification equipment which verifies use rating.
[0002]
[Description of the Prior Art] Along with network progress, the intellectual property expressed by the digital information of software, multimedia data, etc. is increasing by leaps and bounds. and even if reproducing simply comes out of digital information and it copies unjustly, a trace does not remain at all. For this reason, protection of the copyright about digital information poses a problem.
[0003] A ticket is one of those which are daily used as a thing showing the right of use, and digitization of a ticket is also tried. However, there is the same problem as the above-mentioned protection of copyrights.
[0004] As a Prior art which verifies use rating of software, there is a technique currently indicated on the U.S. Pat. No. 5,586,186 number specifications. (It is hereafter called the conventional technique.) Although this technique realizes the access control of software, it can be used also for digitization of a ticket by checking use rating by the enciphered given information being decoded correctly instead of decoding the enciphered software.
[0005] With the conventional technique, it distributed, where software is enciphered, and when a user wishes use of this software, the approach of purchasing the information (user key) for decoding from a software vendor is taken. RSA (Rivest-Shamir-Adleman) public key encryption is used for encryption, and the value acquired by performing a predetermined operation is used for the private key and user identification information of a RSA public key pair as a user key.
[0006]
[Description of the Prior Art] Since the conventional technique is the authentication method of the RSA base, there is much computational complexity. BruceSchneier and Applied according to Cryptography (Second Edition), Wiley, and 1996 -- a workstation (SPARC2) -- law -- as for the time amount which processes 1024-bit data using the RSA cryptosystem of number 1024 bit and, and 8 bits of public keys, as for verification, the signature has taken 0.08 seconds for 0.97 seconds. For this reason, as compared with a workstation like an IC card, there is a problem of taking time amount for authentication, with equipment with little [far] CPU power memory.
[0007]
[Problem(s) to be Solved by the Invention] This invention was made in view of the above-mentioned problem, and makes a technical problem implementation of the use rating verification equipment which can be attested also with equipment with little CPU power memory like an IC card at a high speed.
[0008]
[Means for Solving the Problem] In order to solve said technical problem, the use rating verification equipment of claim 1 has the certification auxiliary information issue section, the verification section, and the certification section. And on the other hand, said certification auxiliary information issue section has the 1st tropism function count means and certification auxiliary information count means calculate certification auxiliary information used for a certification information-management means manage the certification information used in the case of authentication of use rating, the confidential-information management tool which manages secret information, and count of certification auxiliary information, and the 1st means of communications. Moreover, on the other hand, said verification section has the certification information maintenance means [to hold certification

information], trial information count means [to calculate trial information], and 2nd tropism function count means and response indication verification means to verify a response indication, and the 2nd means of communications. Furthermore, on the other hand, said certification section has the confidential information maintenance means [to hold confidential information], certification auxiliary information management means [to manage certification auxiliary information], and 3rd tropism function count means and response indication count means to calculate a response indication, and the 3rd means of communications.

[0009] Moreover, the use rating verification equipment of claim 2 has the certification auxiliary information issue section, the verification section, and the certification section. And on the other hand, said certification auxiliary information issue section has the 1st tropism function count means and certification auxiliary information count means to calculate certification auxiliary information used for a certification information management means to manage certification information, the confidential information management tool which manages secret information, and count of certification auxiliary information, and the 1st means of communications. Moreover, on the other hand, said verification section has the 1st confidential information maintenance means [holding confidential information], 1st certification auxiliary information management means [which manages certification auxiliary information], trial information count means [to calculate trial information], and 2nd tropism function count means and response indication verification means to verify a response indication, and the 2nd means of communications. Furthermore, on the other hand, said certification section has the 2nd confidential information maintenance means [holding confidential information], 2nd certification auxiliary information management means [which manages certification auxiliary information], and 3rd tropism function count means and response indication count means to calculate a response indication, and the 3rd means of communications.

[0010] The use rating verification equipment of claim 3 is use rating verification equipment of claim 1 thru/or claim 2, it combines with certification information and a certification information-management means manages the use limit description it is the information use conditions are shown, it combines with certification auxiliary information, a certification auxiliary information-management means manages use limit description, and use limit description contains in count of the response indication generated in the certification auxiliary information use at said certification section, and said certification section.

[0011] The use rating verification equipment of claim 4 is use rating verification equipment of claim 1 thru/or claim 3, is equipped with a decode means, and when it judges with there being use rating, it decodes information, using the value acquired from certification information or certification information as a decode key of said decode means.

[0012] The use rating verification equipment of claim 5 is use rating verification equipment of claim 1 thru/or claim 4, it has the hysteresis management tool which manages the hysteresis at the time of use rating verification, and it combines with certification auxiliary information, the 1st certification auxiliary information-management means manages transfer information, and trial information stores said transfer information to a hysteresis management tool including transfer information at the time of use rating verification further.

[0013] The use rating verification equipment of claim 6 has the certification auxiliary information issue section, the verification section, and the certification section. And a certification information management means to manage the certification information which uses said certification auxiliary information issue section in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] It has the confidential information which said confidential information management tool manages, said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, and the 1st means of communications which transmit and receive information in process of count of certification auxiliary information. Moreover, a certification information maintenance means by which said verification section holds certification information and the 1st trial information count means which calculates the 1st trial information, On the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] To the 2nd trial information which received, said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and

calculates the 1st response indication, The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Furthermore, a confidential information maintenance means to hold the information that said certification section is secret, A certification auxiliary information management means to manage the certification auxiliary information that it uses for creation of a response indication, The internal-state management tool which manages the internal state corresponding to certification auxiliary information, and the 2nd trial information count means which calculates trial information, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of the received information, and the confidential information which said confidential information maintenance means holds, To the value acquired based on the certification auxiliary information which said certification auxiliary information management means manages, said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act, The 2nd trial information count means which calculates the 2nd trial information, and part or all of the 1st response indication and the 2nd trial information, To the value acquired based on the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages It has the 3rd [said] result on which the tropism function count means was made to act on the other hand, whether a response indication is equal and the 2nd response indication verification means to inspect, and the 3rd means of communications which transmit and receive information in process of the process of authentication of use rating, and certification auxiliary information count.

[0014] The use rating verification equipment of claim 7 has the certification auxiliary information issue section, the verification section, and the certification section. And a certification information management means to manage the certification information which uses said certification information issue section in the case of authentication of use rating, On the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [the confidential information management tool which manages secret information, and asking for an inverse function from the confidential information which said confidential information management tool manages at least] The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand, The 1st means of communications which transmits and receives information in process of count of certification auxiliary information, and the 1st confidential information maintenance means holding secret information, The 1st certification auxiliary information management means which manages certification auxiliary information, and the 1st trial information count means which calculates the 1st trial information, On the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] To the 2nd trial information which received, said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and calculates the 1st response indication, The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information, It has the 2nd means of communications which transmits and receives information in process of authentication of use rating. Furthermore, the 2nd confidential information maintenance means holding the information that said certification section is secret, The 2nd certification auxiliary information management means which manages the certification auxiliary information that it uses for creation of a response indication, The internal-state management tool which manages the internal state corresponding to certification auxiliary information, and the 2nd trial information count means which calculates trial information, On the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand A tropism function count means, [asking for an inverse function] A part or all of the received information, and the confidential information which said confidential information maintenance means holds, To

the value acquired based on the certification auxiliary information which said certification auxiliary information management means manages, said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act, The 2nd trial information count means which calculates the 2nd trial information, and part or all of the 1st response indication and the 2nd trial information, To the value acquired based on the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages It has the 3rd [said] result on which the tropism function count means was made to act on the other hand, whether a response indication is equal and the 2nd response indication verification means to inspect, and the 3rd means of communications which transmit and receive information in process of the process of authentication of use rating, and certification auxiliary information count.

[0015] The use rating verification equipment of claim 8 is use rating verification equipment of claim 6 thru/or claim 7, it combines with certification information and a certification information-management means manages the use limit description it is the information use conditions are shown, it combines with certification auxiliary information, a certification auxiliary information-management means manages use limit description, and use limit description contains in count of the response indication generated in the certification auxiliary information use at said certification section, and said certification section.

[0016] The use rating verification equipment of claim 9 is use rating verification equipment of claim 6 thru/or claim 8, is equipped with a decode means, and when it judges with there being use rating, it decodes information, using the value acquired from certification information or certification information as a decode key of said decode means.

[0017] The use rating verification equipment of claim 10 is use rating verification equipment of claim 6 thru/or claim 9, it has the hysteresis management tool which manages the hysteresis at the time of use rating verification, and it combines with certification auxiliary information, the 1st certification auxiliary information-management means manages transfer information, and trial information stores said transfer information to a hysteresis management tool including transfer information at the time of use rating verification further.

[0018]

[Function] The use rating verification equipment of this invention performs issue of certification auxiliary information, and verification of use rating.

[0019] In issue of certification auxiliary information, each means carries out the following operations for any use rating verification equipment of a claim.

[0020] The information for identifying what kind of right is published by the 1st means of communications to which device that has a confidential information maintenance means is received. When there is use limit description which restricts this right in a period etc., it is collectively specified by use limit description at this time.

[0021] A confidential information management tool searches the confidential information which the confidential information maintenance means of this device holds from the information which identifies a device.

[0022] A certification information management means retrieves the certification information corresponding to this right from the information which identifies a right. On the other hand, at least, to this confidential information and this right identification information, while the 1st thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function. When use limit description exists, on the other hand, a tropism function is applied also including use limit description.

[0023] A certification auxiliary information count means calculates certification auxiliary information based on this certification information and the value acquired as a result of applying a tropism function on the other hand.

[0024] It is transmitted from the 1st means of communications, and this certification auxiliary information is transmitted to the means of communications of this device, and is stored in the certification auxiliary information management means of this device.

[0025] The operation in verification of use rating in the use rating verification equipment of claim 1 is as follows.

[0026] A trial information count means generates a random number, combines with this random number the identification information of the right which a certification information maintenance means holds, and makes it trial information.
[0027] This trial information is transmitted to the 3rd means of communications from the 2nd means of communications. A certification auxiliary information management means retrieves the certification auxiliary information corresponding to the identification information of the right contained in this trial information.
[0028] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0029] A response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information. On the other hand, to the random number of this certification information and this trial information, while the 3rd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function, and it makes it a response indication.
[0030] The 3rd means of communications transmits a response indication to the 2nd means of communications.
[0031] On the other hand, to the random number of this certification information and this trial information, while the 2nd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function.
[0032] The response indication verification section judges with what, on the other hand, compares the application result and this response indication of a tropism function, restricts when [said] in agreement, and has use rating.
[0033] The operation in verification of use rating in the use rating verification equipment of claim 2 is as follows.
[0034] In advance of verification of use rating, it is determined which right is verified whether the identification information of a right is inputted from the 2nd means of communications, and by calculating according to the regulation set to beforehand.
[0035] A trial information count means generates a random number, combines the identification information of this right with this random number, and makes it trial information.
[0036] This trial information is transmitted to the 3rd means of communications from the 2nd means of communications. The 2nd certification auxiliary information management means retrieves the certification auxiliary information corresponding to the identification information of the right contained in this trial information.
[0037] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0038] A response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information.
[0039] On the other hand, to the random number of this certification information and this trial information, while the 3rd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function, and it makes it a response indication.
[0040] The 3rd means of communications transmits a response indication to the 2nd means of communications.
[0041] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 2nd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0042] A response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information.
[0043] On the other hand, to the random number of this certification information and this trial information, while the 2nd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function.
[0044] The response indication verification section judges with what, on the other hand, compares the application result and this response indication of a tropism function, restricts when [said] in agreement, and has use rating.

[0045] The operation in verification of use rating in the use rating verification equipment of claim 3 is as follows.
[0046] This use rating verification equipment is equipped with the same means as the use rating verification equipment of claim 1 thru/or claim 2.
[0047] In case use ****** is combined with certification auxiliary information, and a certification auxiliary information management means to manage the certification auxiliary information that it uses for count of a response indication manages it and retrieves certification auxiliary information from the identification information of a right, it also searches use limit description to coincidence.
[0048] On the other hand, to the 3rd confidential information which this right identification information, this use limit description, and a confidential information maintenance means hold, while a tropism function count means is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function.
[0049] A response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information. On the other hand, to the random number of this certification information and this trial information, and this use limit description, while the 3rd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function. This use limit description and the value acquired here are combined, and it considers as a response indication.
[0050] A response indication verification means judges as what restricts when the 1st value which, on the other hand, applied the tropism function count means, and information other than use limit description of this response indication are in agreement and use limit description fulfills predetermined conditions to use limit description of the random number of certification information and this trial information, and this response indication, and has use rating. (Whether predetermined conditions' being fulfilled and the approach of judging also have use limit description with a response indication count means.)
The operation in verification of use rating in the use rating verification equipment of claim 4 is as follows.
[0051] This use rating verification equipment is equipped with the same means as the use rating verification equipment of claim 1 thru/or claim 3.
[0052] With a response indication verification means, when judged with a thing with use rating, information is decoded, using the value acquired from certification information or certification information by the decode means as a decode key of said decode means.
[0053] The operation in verification of use rating in the use rating verification equipment of claim 5 is as follows.
[0054] This use rating verification equipment is equipped with the same means as the use rating verification equipment of claim 1 thru/or claim 4.
[0055] Transfer information is combined with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information management means manages it.
[0056] Trial information includes this transfer information further.
[0057] Said transfer information is stored in a hysteresis management tool at the time of use rating verification.
[0058] The operation in verification of use rating in the use rating verification equipment of claim 6 is as follows.
[0059] The 1st trial information count means generates the 1st random number, combines with this random number at least the identification information of the right which a certification information maintenance means holds, and makes it trial information.
[0060] This trial information is transmitted to the 3rd means of communications from the 2nd means of communications.
[0061] The 2nd trial information count means generates the 2nd random number, and makes this the 2nd trial information.
[0062] The 3rd means of communications transmits the 2nd trial information to the 2nd means of communications. The 1st response indication count means makes information which includes at least the 2nd value which inputted into the tropism function count means on the other hand, and was acquired here for the 2nd trial information the 1st response indication.

[0063] The 1st response indication is transmitted to the 3rd means of communications from the 2nd means of communications. A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0064] A certification auxiliary information management means retrieves the certification auxiliary information corresponding to the identification information of the right contained in this trial information.
[0065] The 2nd response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information. Subsequently, the 1st response indication compares the 3rd value acquired with the application of a tropism function count means on the other hand to information including the 2nd trial information and this certification information.
[0066] If a value does not fill predetermined relation, a meaningless value is generated, it considers as the 2nd response indication and predetermined relation is filled, modification of the below-mentioned internal state and count of a response indication will be performed.
[0067] An internal-state management tool searches the internal state corresponding to this right identification information, and changes this internal state according to the information transmitted by the 1st trial information or 1st response indication.
[0068] On the other hand, to the 3rd random number [1st] contained in this certification information and the 1st trial information, while a tropism function count means is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function.
[0069] The 2nd response indication count means makes this value the 2nd response indication.
[0070] The 3rd means of communications transmits a response indication to the 2nd means of communications.
[0071] On the other hand, to the random number of this certification information and this trial information, while the 2nd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function.
[0072] The response indication verification section judges with what, on the other hand, compares the application result and this response indication of a tropism function, restricts when [said] in agreement, and has use rating.
[0073] The operation in verification of use rating in the use rating verification equipment of claim 7 is as follows.
[0074] In advance of verification of use rating, it is determined which right is verified whether the identification information of a right is inputted from the 2nd means of communications, and by calculating according to the regulation set to beforehand.
[0075] A trial information count means generates a random number, combines the identification information of this right with this random number, and makes it trial information.
[0076] This trial information is transmitted to the 3rd means of communications from the 2nd means of communications. The 1st certification auxiliary information management means retrieves the certification auxiliary information corresponding to the identification information of the right contained in this trial information.
[0077] The 1st trial information count means generates the 1st random number, combines with this random number at least the identification information of the right which a certification information maintenance means holds, and makes it trial information. This trial information is transmitted to the 3rd means of communications from the 2nd means of communications. The 2nd trial information count means generates the 2nd random number, and makes this the 2nd trial information.
[0078] The 3rd means of communications transmits the 2nd trial information to the 2nd means of communications. A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 2nd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0079] The 1st response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information.
[0080] The 1st response indication count means makes information which includes at least the 2nd value which inputted into the tropism function count means on the other hand, and was acquired here for this certification

information and the 2nd trial information the 1st response indication.
[0081] The 1st response indication is transmitted to the 3rd means of communications from the 2nd means of communications. A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which a confidential information maintenance means, on the other hand, holds a tropism function count means, and this right identification information.
[0082] A certification auxiliary information management means retrieves the certification auxiliary information corresponding to the identification information of the right contained in this trial information.
[0083] The 2nd response indication count means calculates the count result of the aforementioned one direction nature function, and this certification auxiliary information, and searches for certification information. Subsequently, the 1st response indication compares the 3rd value acquired with the application of a tropism function count means on the other hand to information including the 2nd trial information and this certification information.
[0084] If a value does not fill predetermined relation, a meaningless value is generated, it considers as the 2nd response indication and predetermined relation is filled, modification of the below-mentioned internal state and count of a response indication will be performed.
[0085] An internal-state management tool searches the internal state corresponding to this right identification information, and changes this internal state according to the information transmitted by the 1st trial information or 1st response indication.
[0086] On the other hand, to the 3rd random number [1st] contained in this certification information and the 1st trial information, while a tropism function count means is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function.
[0087] The 2nd response indication count means makes this value the 2nd response indication.
[0088] The 3rd means of communications transmits a response indication to the 2nd means of communications.
[0089] On the other hand, to the random number of this certification information and this trial information, while the 2nd thing to search for for an inverse function is difficult for a tropism function count means in computational complexity at least, it applies a tropism function.
[0090] The response indication verification section judges with what, on the other hand, compares the application result and this response indication of a tropism function, restricts when [said] in agreement, and has use rating.
[0091] The operation in verification of use rating in the use rating verification equipment of claim 10 is as follows.
[0092] This use rating verification equipment is equipped with the same means as the use rating verification equipment of claim 6 thru/or claim 9.
[0093] Transfer information is combined with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information management means manages it.
[0094] The 1st trial information or 1st response indication includes this transfer information further.
[0095] Said transfer information is stored in a hysteresis management tool at the time of use rating verification.
[0096]
[The mode of implementation of invention] Each use rating verification equipment of the example described below consists of three elements, a certification auxiliary information issue machine, a verification machine, and a certification machine.
[0097] A certification auxiliary information issue machine publishes certification auxiliary information that it uses in process of verification of use rating.
[0098] A verification machine and a certification machine perform dialogue certification, and verify the existence of use rating. In little [far] MD5, SHA, etc., on the other hand in the process of dialogue certification, computational complexity uses a tropism function compared with a public-key-encryption system. Although what, on the other hand, takes two or more arguments as a tropism function is used in the following examples, MD5 and SHA can be used by connecting the bit string of each argument.
[0099] In addition, the correspondence relation between the example of the user rating verification equipment explained below and a claim is as follows, and explains each example with reference to corresponding drawing. In addition, drawing 1 - drawing 8 show the configuration of each example, and drawing 9 and drawing 10

show actuation.
[0100]
[Table 1]
The 1st example Claim 1 The 2nd example of drawing 1 Claim 2 The 3rd example of drawing 2 Claim 3 The 4th example of drawing 2 Claim 4 The 5th example of drawing 3 Claim 5 Drawing 4 , the 6th example of drawing 9 Claim 6 The 7th example of drawing 5 Claim 7 The 8th example of drawing 6 The 9th example of claim 8 drawing 6 The 10th example of claim 9 drawing 7 Claim 10 Drawing 8 , drawing 10 [0101] The 1st example is explained below the [1st example]. On the other hand, this example performs fundamental dialogue authentication using a tropism function.
[0102] Drawing 1 shows the configuration of the 1st example and use rating verification equipment contains the certification auxiliary information issue machine 10, the verification machine 20, and the certification machine 30 in this drawing. The certification auxiliary information issue machine 10 publishes certification auxiliary information in the certification vessel 20. The certification machine 30 uses this certification auxiliary information, and is a deed about dialogue authentication between the verification machines 20. If authentication is successful, the program execution section 40 will perform a program.
[0103] The certification auxiliary information issue machine 10 is constituted including the 1st communications department 101, the confidential information Management Department 102, the certification Research and Data Processing Department 103, the 1st one direction nature count section 104, and the certification auxiliary information count section 105.
[0104] The flow of processing of the certification auxiliary information issue machine 10 is shown in drawing 1111 .
[0105] This certification auxiliary information issue machine 10 publishes certification auxiliary information based on the demand from the certification machine 30. The 1st communications department 101 receives the identification information of certification equipment 30, and the information for identifying what kind of right is published from the certification machine 30 (S11, S12 of drawing 11). The confidential information Management Department 102 searches the confidential information which certification equipment 30 holds from the information which identifies certification equipment 30 (S13). The certification Research and Data Processing Department 103 retrieves the certification information (K) corresponding to this right from the information which identifies a right. On the other hand, at least, to confidential information and right identification information, while the 1st thing to search for for an inverse function is difficult for the tropism function count section 104 in computational complexity at least, it applies a tropism function. The certification auxiliary information count section 105 calculates certification auxiliary information based on certification information and the value acquired as a result of applying a tropism function on the other hand (S14). This certification auxiliary information is transmitted to the certification machine 30 from the 1st communications department 101 (S15).
[0106] The verification machine 20 is constituted including the certification information attaching part 201, the trial information count section 202, the 2nd one direction nature function count section 203, the response indication verification machine 204, and the 2nd communications department 205.
[0107] The verification machine 20 verifies the certification information to which trial information is returned by the certification machine 30 from delivery and the certification machine 30, and performs dialogue authentication between certification equipment.
[0108] The flow of processing of the verification machine 20 is shown in drawing 12 .
[0109] The certification information attaching part 201 holds the identification information of a right. The trial information count section 202 generates a random number, combines a random number and the identification information of the right which the certification information attaching part 201 holds, and is taken as trial information (S21 of drawing 12). This trial information is transmitted to the 3rd communications department 305 of the certification machine 30 from the 2nd communications department 205 (S22). Moreover, the 2nd communications department 205 receives the response indication returned from the certification machine 30 (S23). On the other hand, to the random number of certification information and this trial information, while the 2nd thing to search for for an inverse function is difficult for the tropism function count section 203 in computational complexity at least, it applies a tropism function. The response indication verification machine 204 is judged to be what, on the other hand, compares the application result of a tropism function with a

response indication, restricts when in agreement, and has use rating (S24, S25).
[0110] The certification machine 30 is constituted including the confidential information attaching part 301, the certification auxiliary Research and Data Processing Department 302, the response indication count section 303, the 3rd one direction nature function count section 304, and the 3rd communications department 305.
[0111] The certification machine 30 performs predetermined count to the trial information sent from the verification machine 20, generates a response indication, and returns it to the verification machine 20.
[0112] The flow of processing of the certification machine 30 is shown in drawing 13 .
[0113] Trial information is transmitted to the 3rd communications department 305 from the 2nd communications department 205 (S31).
[0114] The confidential information attaching part 301 holds the confidential information of a proper in the certification vessel 30. The certification auxiliary Research and Data Processing Department 302 retrieves the certification auxiliary information corresponding to the identification information of the right contained in trial information (S32). Certification auxiliary information has come to hand from the certification auxiliary information issue machine 10 beforehand. A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which the confidential information attaching part 301, on the other hand, holds the tropism function count section 304, and the right identification information contained in trial information (S33). On the other hand, the response indication count section 303 calculates the count result and certification auxiliary information on a tropism function, and searches for certification information. Furthermore, to the 3rd random number contained in certification information and trial information, while the tropism function count section 304 is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function, and on the other hand, it is taken as a response indication. This response indication is sent to the 2nd communications department 205 of the verification machine 20 through the 3rd communications department 305 (S34, S35).
[0115] Hereafter, the protocol of authentication of the 1st example is explained to a detail.
[0116] In the 1st example, the certification auxiliary information t is defined as follows.
[0117]
[Equation 1] t=K-f(d,n)
It is the information which identifies the right to which certification information and f should verify K and confidential information and n should verify a tropism function and d on the other hand here. The trial information C sent to the certification machine 30 from the verification machine 20 uses r as a random number, and is [0118].
[Equation 2] It is C= (n, r).
[0119] The certification machine 30 searches for a response indication R by the following count.
[0120]
[Equation 3] R=f(t+f(d,n),r)
It is [0121] when the certification machine 30 holds the right certification auxiliary information t.
[Equation 4] It is set to t+f(d, n) =K-f(d, n)+f(d, n) =K, the certification information K can be restored, and it is [0122].
[Equation 5] R=f(K,r)
It becomes.
[0123] the verification machine 20 -- f (K, r) -- asking -- a response indication R -- comparing -- case both are equal -- as long as -- a certification machine judges with what has use rating.
[0124] [Example which is the 2nd] The 2nd example is explained below. This example decides beforehand about those with two or more, and which right the right for authentication attests. Which right is attested inputs the identification information of a right, or it is calculated and determined under the regulation defined beforehand. On the other hand, the base of the authentication technique using a tropism function is the same as the 1st example.
[0125] Drawing 2 shows the configuration of the 2nd example and gave the corresponding sign to drawing 1 and a corresponding part in this drawing.
[0126] The certification auxiliary information issue machine 10 of this example publishes certification auxiliary information that answer the demand of the verification machine 10 and the certification machine 20, respectively, and it corresponds to it.

[0127] The verification machine 20 has the 1st confidential information attaching part 206 and the 1st certification auxiliary Research and Data Processing Department 207. The certification machine 30 has the 2nd confidential information attaching part 306 and the 2nd certification auxiliary Research and Data Processing Department 307.
[0128] First, in advance of verification of use rating, the identification information of a right is inputted through the 2nd communications department 205, and it is determined which right is verified. This decision may be made by calculating according to the regulation defined in advance.
[0129] The trial information count section 202 generates a random number, combines the identification information of a right with a random number, and is taken as trial information. This trial information is transmitted to the 3rd communications department 305 of the certification machine 30 from the 2nd communications department 205.
[0130] The 2nd certification auxiliary Research and Data Processing Department 307 of the certification machine 30 retrieves the certification auxiliary information corresponding to the identification information of the right contained in trial information. And a tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which the 2nd confidential information attaching part 306, on the other hand, holds the tropism function count section 304, and right identification information. Furthermore, on the other hand, the response indication count section 303 calculates the count result and certification auxiliary information on a tropism function, and searches for certification information. On the other hand, further, to the random number of certification information and this trial information, while the 3rd thing to search for for an inverse function is difficult for the tropism function count section 304 in computational complexity at least, it applies a tropism function, and it is taken as a response indication. This response indication is sent to the verification machine 20 through the 3rd communications department 305 and 2nd communications department 205.
[0131] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 2nd confidential information to which the 1st confidential information attaching part 206, on the other hand, holds the tropism function count section 203 and right identification information of the verification machine 20. And on the other hand, a predetermined operation is performed to the count result and certification auxiliary information on a tropism function, and certification information is searched for. On the other hand, further, to the random number of certification information and trial information, while the 2nd thing to search for for an inverse function is difficult for the tropism function count section 203 in computational complexity at least, it applies a tropism function. The response indication verification machine 204 is judged to be what, on the other hand, compares the application result of a tropism function with a response indication, restricts when in agreement, and has use rating.
[0132] Below, the Challenge Handshake Authentication Protocol of the 2nd example is explained to a detail.
[0133] In the 2nd example, the certification auxiliary information tv on a verification machine and the certification auxiliary information tp on a certification machine are defined as follows.
[0134]
[Equation 6]
$tv=K-f(dv,n)$
$tp=K-f(dp,n)$
Here, K is information which identifies the right to which a tropism function and dv should verify certification information and f, and the confidential information of the certification machine 30 and n should, on the other hand, verify the confidential information of the verification machine 20, and dp.
[0135] The trial information C sent to the certification machine 30 from the verification machine 20 uses r as a random number, and is [0136].
[Equation 7] $C=(n,r)$
It comes out.
[0137] The certification machine 30 searches for a response indication R by the following count.
[0138]
[Equation 8] $R=f(tp+f(dp,n),r)$
It is [0139] when the certification machine 30 holds the right certification auxiliary information tp.
[Equation 9] It is set to $tp+f(dp, n) =K-f(dp, n)+f(dp, n) =K$, the certification information K can be restored, and

it is [0140].
[Equation 10] R=f(K,r)
It becomes.
[0141] The verification machine 20 calculates tv+f (dv, n), and asks for K. subsequently, f (K, r) -- asking -- R -- comparing -- case both are equal -- as long as -- a certification machine judges with what has use rating.
[0142] [Example which is the 3rd] The 3rd example is explained below. This example introduces a use limit further in the 2nd example.
[0143] The configuration of the 3rd example itself is the same as that of the 2nd example, and it is as being shown in drawing 2 .
[0144] Hereafter, the Challenge Handshake Authentication Protocol of the 3rd example is explained.
[0145] In the 3rd example, the certification auxiliary information tv on the verification machine 20 and the certification auxiliary information tp on the certification machine 30 are defined as follows.
[0146]
[Equation 11]
tv=K-f(dv,n)
tp=K-f(dp,n,L)
The information and L from which K discriminates the right to which a tropism function and dv should verify certification information and f, and the confidential information of the verification machine 20 and dp should, on the other hand, verify the confidential information of the certification machine 30 and n here are use limit description. The use limit description L is a bit string showing the expiration date.
[0147] The trial information C sent to the certification machine 30 from the verification machine 20 uses r as a random number, and is [0148].
[Equation 12] C=(n,r)
It comes out.
[0149] The certification machine 30 searches for a response indication R by the following count.
[0150]
[Equation 13]
R=(L,f(tp+f(dp,n,L),r,L))
It is [0151] when the certification machine 30 holds the right certification auxiliary information tp.
[Equation 14] It is set to tp+f(dp, n, L) =K-f(dp, n, L)+f(dp, n, L) =K, the certification information K can be restored, and it is [0152].
[Equation 15] R=(L,f(K,r,L))
It becomes.
[0153] The verification machine 20 calculates tv+f (dv, n), and asks for K. Subsequently, it restricts, when ** [both] and the use limit description L fulfill a service condition in quest of f (K, r) as compared with R, and it judges with that in which the certification machine 30 has use rating.
[0154] Although it shall judge whether the use limit description L fulfills a service condition with the verification vessel 20 here, the certification machine 30 may be made to perform. It is not necessary to include the use limit description L in a response indication at this time.
[0155] [Example which is the 4th] The 4th example is explained below. This example decodes the information enciphered considering the value drawn from the certification information K or certification information as a key.
[0156] Drawing 3 shows the configuration of the 4th example and gave the corresponding sign to the corresponding part with drawing 2 in this drawing. In this example, the decode section 208 is added to the verification machine 20.
[0157] The information and the verification procedure which are treated in the 4th example are the same as the 3rd example. When the decode section 208 of the verification machine 20 is judged as the certification machine 30 having use rating, the information which used the certification information K and K and was enciphered, using a computable value as a key is decoded.
[0158] [Example which is the 5th] The 5th example is explained below. This example enables it to manage use hysteresis.
[0159] Drawing 4 shows the configuration of the 5th example and gave the corresponding sign to drawing 3 and

a corresponding part in this drawing. In drawing 4 , the hysteresis Management Department 308 is established in the certification machine 30.
[0160] Hereafter, the Challenge Handshake Authentication Protocol of the 5th example is explained.
[0161] This authentication procedure is shown also in drawing 9 . Since each actuation of the 4th of the 1st - an example is included in the 5th example, it can also understand actuation of the 4th of the 1st - an example from drawing 9 .
[0162] Hereafter, the Challenge Handshake Authentication Protocol of the 5th example is explained to a detail.
[0163] In the 5th example, the certification auxiliary information tv on the verification machine 20 and the certification auxiliary information tp on the certification machine 30 are defined as follows.
[0164]
[Equation 16]
tv=K-f(dv,n)
tp=K-f(dp,n,L)
The information and L from which K discriminates the right to which a tropism function and dv should verify certification information and f, and the confidential information of the verification machine 20 and dp should, on the other hand, verify the confidential information of the certification machine 30 and n here are use limit description. The use limit description L is a bit string showing the expiration date.
[0165] The verification machine 20 calculates tv+f (dv, n), and asks for K.
[0166] The trial information C sent to the certification machine 30 from the verification machine 20 uses r as a random number, and is [0167].
[Equation 17] C=(n,I,r,s)
It comes out. Here, the information and s which transmit I to the certification machine 30 from the verification machine 20 are [0168].
[Equation 18] s=f(K,I,r)
It is the becoming value. The certification machine 30 asks for K' by the following count.
[0169]
[Equation 19] K'=tp+f(dp,n,L)
Subsequently, f (K', I, r) is calculated and it compares with s. It restricts, when s is in agreement, and the information containing I is stored in the hysteresis attaching part 308.
[0170] The certification machine 30 searches for a response indication R further.
[0171]
[Equation 20]
R=(L,f(tp+f(dp,n,L),r,L))
It is [0172] when the certification machine 30 holds the right certification auxiliary information tp.
[Equation 21] It is set to tp+f(dp, n, L) =K-f(dp, n, L)+f(dp, n, L) =K, the certification information K can be restored, and it is [0173].
[Equation 22] R=(L,f(K,r,L))
It becomes.
[0174] Subsequently, it restricts, when ** [both] and L fulfill a service condition in quest of f (K, r) as compared with R, and it judges with that in which a certification machine has use rating.
[0175] Here, although it shall judge whether the use limit description L fulfills a service condition with the verification vessel 20, the certification machine 30 may be made to perform.
[0176] [Example which is the 6th] The 6th example is explained below. The 6th example performs mutual recognition and enables it to change the internal state of the certification machine 30.
[0177] Drawing 6 shows the configuration of the 6th example and gave the corresponding sign to drawing 1 and a corresponding part in this drawing. In drawing 6 , the 1st trial information count section 209, the 1st response indication count section 210, and the 1st response indication verification machine 211 were formed in the verification machine 20, and the 2nd trial information count section 309, the 2nd response indication count section 310, the 2nd response indication verification machine 311, and the internal-state Management Department 312 are established in the certification machine 30.
[0178] In this example, in process of dialogue authentication, each attests, the verification machine 20 performs decode etc. and the certification machine 30 changes the internal state corresponding to decode etc.

[0179] The flow of processing of the verification machine 20 of this example and the certification machine 30 is shown in drawing 14 and drawing 15 , respectively.
[0180] The 1st trial information count section 209 of the verification machine 20 generates the 1st random number, combines at least the 1st random number and the identification information of the right which the certification information attaching part 201 holds, and is taken as trial information (S41 of drawing 14). This trial information is transmitted to the 3rd communications department 305 of the certification machine 30 from the 2nd communications department 205 (S42, S51 of drawing 15).
[0181] On the other hand, the 2nd trial information count section 309 generates the 2nd random number, makes this the 2nd trial information, and transmits to the verification machine 20 (the 2nd communications department 205) through the 3rd communications department 305 (S52, S43).
[0182] The 1st response indication count section 210 of the verification machine 20 generates the 1st response indication so that the information itself to deliver at least the 2nd trial information and the information transmitted to the certification machine 30 from the verification machine 20 the 2nd value which inputted into the tropism function count section 203 on the other hand, and was acquired here may be included. This 1st response indication is transmitted to the 3rd communications department 305 of the certification machine 30 from the 2nd communications department 205 (S44, S53).
[0183] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which the confidential information attaching part 301, on the other hand, holds the tropism function count section 304 and right identification information of the certification machine 30.
[0184] The certification auxiliary Research and Data Processing Department 302 retrieves the certification auxiliary information corresponding to the identification information of the right contained in trial information (S54).
[0185] On the other hand, the 2nd response indication count section 310 calculates the count result and certification auxiliary information on a tropism function, and searches for certification information. Subsequently, the 3rd value which, on the other hand, applied the tropism function count section 304, and was acquired as a result, and the 1st response indication (that part) are collated to the 2nd trial information and information including certification information (S55, S56). If a value does not fill predetermined relation, a meaningless value is generated, it considers as the 2nd response indication and predetermined relation is filled, modification of the below-mentioned internal state and count of a response indication will be performed.
[0186] The internal-state Management Department 312 searches the internal state corresponding to right identification information, and changes an internal state according to the information transmitted by the 1st trial information or 1st response indication.
[0187] On the other hand, to the 3rd random number [1st] contained in certification information and the 1st trial information, while the tropism function count section 304 is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function, and the 2nd response indication count section 311 makes this value the 2nd response indication. The 3rd communications department 305 transmits the 2nd response indication to the communications department 205 of the 2nd verification machine 20 (S57, S58, S45).
[0188] On the other hand, to the random number of certification information and trial information, while the 2nd [of the verification machine 20] thing to search for for an inverse function is difficult for the tropism function count section 203 in computational complexity at least, it applies a tropism function. The 1st response indication verification machine 211 is judged to be what, on the other hand, compares the application result of a tropism function with the 2nd response indication, restricts when in agreement, and has use rating (S46, S47).
[0189] Hereafter, the protocol of authentication of the 6th example is explained.
[0190] In the 6th example, the certification auxiliary information t is defined as follows.
[0191]
[Equation 23] $t=K-f(d,n)$
It is the information which identifies the right to which certification information and f should verify K and confidential information and n should verify a tropism function and d on the other hand here.
[0192] The 1st trial information C1 sent to the certification machine 30 from the verification machine 20 uses r1 as a random number, and is [0193].
[Equation 24] $C1=(n,r1)$

It comes out.
[0194] The certification machine 30 sends the 2nd trial information C2 to the verification machine 20.
[0195]
[Equation 25] C2=r2 -- here, r2 is a random number.
[0196] The verification machine 20 sends the 1st response indication R1 to the certification machine 30.
[0197]
[Equation 26] R1=(m,f(K,r2,m))
Here, m is information transmitted to the certification machine 30 from the verification machine 20. m is a frame charged at every use.
[0198] The certification machine 30 asks for K' by the following count.
[0199]
[Equation 27] K'=tp+f(dp,n)
The certification auxiliary information tp of K' corresponds with the certification information K at a right case.
[0200] The certification machine 30 calculates f (K', r2, m), and compares it with the 2nd term of R1. When both are equal, according to the information m transmitted from the verification machine 20, the internal state corresponding to the right which should be verified is changed. For example, if it is the frame charged whenever m is use, a prepaid frame will be reduced a ****ed part.
[0201] Subsequently, the certification machine 30 searches for the 2nd response indication R2.
[0202]
[Equation 28] R2=f(K',r1)
When the certification machine holds the right certification auxiliary information tp, K' is in agreement with the certification information K, and it is [0203].
[Equation 29] R2=f(K,r)
It becomes.
[0204] the verification machine 20 -- f (K, r) -- asking -- R2 -- comparing -- case both are equal -- as long as -- the certification machine 30 judges with what has use rating.
[0205] [Example which is the 7th] The 7th example is explained below. This example decides beforehand about those with two or more, and which right the right for authentication attests. Which right is attested inputs the identification information of a right, or it is calculated and determined under the regulation defined beforehand. Other configurations are the same as that of the 6th example.
[0206] In addition to the configuration of the 6th example (drawing 5), the verification machine 20 of this example has formed the 1st confidential information attaching part 206 and the 1st certification auxiliary Research and Data Processing Department 207. Moreover, the certification machine 30 has the 2nd confidential information attaching part 306 (confidential information attaching part 301 of drawing 5), and the 2nd certification auxiliary Research and Data Processing Department 307 (confidential information attaching part 302 of drawing 5). In drawing 6 , the corresponding sign was given to drawing 5 and a corresponding part.
[0207] The certification auxiliary information issue machine 10 of this example publishes certification auxiliary information that answer the demand of the verification machine 10 and the certification machine 20, respectively, and it corresponds to it.
[0208] In advance of verification of use rating, it is determined which right is verified whether the identification information of a right is inputted from the 2nd communications department 205, and by calculating according to the regulation set to beforehand.
[0209] The 1st certification auxiliary Research and Data Processing Department 207 of the verification machine 20 retrieves the certification auxiliary information corresponding to the identification information of the right contained in trial information.
[0210] The 1st trial information count section 209 generates the 1st random number, combines a random number and the identification information of a right at least, and is taken as trial information. This trial information is transmitted to the 3rd communications department 305 of the certification machine 30 from the 2nd communications department 205.
[0211] The 2nd trial information count section 309 of the certification machine 30 generates the 2nd random number, and makes this the 2nd trial information. The 3rd communications department 305 transmits the 2nd trial information to the 2nd communications department 205 of the verification machine 20.

[0212] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 2nd confidential information to which the confidential information attaching part 206, on the other hand, holds the tropism function count section 203 and right identification information of the verification machine 20.
[0213] On the other hand, the 1st response indication count section 210 calculates the count result and certification auxiliary information on a tropism function, and searches for certification information. The 1st response indication count section 210 generates the 1st response indication like with the information itself which delivered at least the 2nd trial information and the information transmitted to the certification machine 30 from the verification machine 20 the 2nd value which inputted into the tropism function count section on the other hand, and was acquired here. This 1st response indication is transmitted to the 3rd communications department 305 from the 2nd communications department 205.
[0214] A tropism function is applied while it is difficult in computational complexity at least to ask for an inverse function from the 3rd confidential information to which the 2nd confidential information attaching part 206, on the other hand, holds the tropism function count section 304 and right identification information of the certification machine 30.
[0215] The 2nd certification auxiliary Research and Data Processing Department 307 retrieves the certification auxiliary information corresponding to the identification information of the right contained in trial information.
[0216] On the other hand, the 2nd response indication count section 310 calculates the count result and certification auxiliary information on a tropism function, and searches for certification information. Subsequently, the 1st response indication collates the 3rd value acquired with the application of the tropism function count section on the other hand, and the 1st response indication (the part) to information including the 2nd trial information and certification information. If a value does not fill predetermined relation, a meaningless value is generated, it considers as the 2nd response indication and predetermined relation is filled, modification of the below-mentioned internal state and count of a response indication will be performed.
[0217] The internal-state Management Department 312 searches the internal state corresponding to right identification information, and changes an internal state according to the information transmitted by the 1st trial information or 1st response indication.
[0218] On the other hand, to the 3rd random number [1st] contained in certification information and the 1st trial information, while the tropism function count section 304 is difficult to ask for an inverse function in computational complexity at least, it applies a tropism function, and the 2nd response indication count section 310 makes this value the 2nd response indication. The 3rd communications department 305 transmits a response indication to the 2nd communications department 205.
[0219] On the other hand, to the random number of certification information and trial information, while the 2nd [of the verification machine 20] thing to search for for an inverse function is difficult for the tropism function count section 203 in computational complexity at least, it applies a tropism function.
[0220] The 1st response indication verification machine 211 is judged to be what, on the other hand, compares the application result of a tropism function with the 2nd response indication, restricts when in agreement, and has use rating.
[0221] Hereafter, the Challenge Handshake Authentication Protocol of the 7th example is explained.
[0222] In the 7th example, the certification auxiliary information tv on a verification machine and the certification auxiliary information tp on a certification machine are defined as follows.
[0223]
[Equation 30]
tv=K-f(dv,n)
tp=K-f(dp,n)
Here, K is information which identifies the right to which a tropism function and dv should verify certification information and f, and the confidential information of a certification machine and n should, on the other hand, verify the confidential information of a verification machine, and dp.
[0224] The 1st trial information C1 sent to the certification machine 30 from the verification machine 20 uses r1 as a random number, and is [0225].
[Equation 31] C1=(n,r1)
It comes out.

[0226] 30 certification machine sends the 2nd trial information C2 to the verification machine 20.
[0227]
[Equation 32] C2=r2 -- here, r2 is a random number.
[0228] The verification machine 20 calculates tv+f (dv, n), and asks for K. Subsequently, the 1st response indication R1 is searched for by the following count.
[0229]
[Equation 33] R1=(m,f(K,r2,m))
Here, m is information transmitted to the certification machine 30 from the verification machine 20.
[0230] The certification machine 30 asks for K' by the following count.
[0231]
[Equation 34] K'=tp+f(dp,n)
The certification auxiliary information tp of K' corresponds with the certification information K at a right case.
[0232] The certification machine 30 calculates f (K', r2, m), and compares it with the 2nd term of R1. When both are equal, according to the information m transmitted from the verification machine 20, the internal state corresponding to the right which should be verified is changed. For example, if it is the frame charged whenever m is use, a prepaid frame will be reduced a ****ed part.
[0233] Subsequently, the certification machine 30 searches for the 2nd response indication R2.
[0234]
[Equation 35] R2=f(K',r1)
When the certification machine holds the right certification auxiliary information tp, K' is in agreement with the certification information K, and it is [0235].
[Equation 36] R2=f(K,r)
It becomes.
[0236] the verification machine 20 -- f (K, r) -- asking -- R2 -- comparing -- case both are equal -- as long as -- the certification machine 30 judges with what has use rating.
[Example which is the 8th] The 8th example is explained below. The 8th example introduces use limit information in the 7th example. The configuration of the 8th example is constituted as shown in drawing 6 like the 7th example.
[0237] Hereafter, the Challenge Handshake Authentication Protocol of the 8th example is explained.
[0238] In the 8th example, the certification auxiliary information tv on the verification machine 20 and the certification auxiliary information tp on the certification machine 30 are defined as follows.
[0239]
[Equation 37]
tv=K-f(dv,n)
tp=K-f(dp,n,L)
The information and L from which K discriminates the right to which a tropism function and dv should verify certification information and f, and the confidential information of the verification machine 20 and dp should, on the other hand, verify the confidential information of the certification machine 30 and n here are use limit description.
[0240] The 1st trial information C1 sent to the certification machine 30 from the verification machine 20 uses r1 as a random number, and is [0241].
[Equation 38] C1=(n,r1)
It comes out.
[0242] The 2nd trial information C2 sent to the verification machine 20 from the certification machine 30 uses r2 as a random number, and is [0243].
[Equation 39] It is C2=r2.
[0244] The verification machine 20 calculates tv+f (dv, n), and asks for K. Subsequently, the 1st response indication R1 is searched for by the following count.
[0245]
[Equation 40] R1=(m,f(K,r2,m))
Here, m is information transmitted to the certification machine 30 from the verification machine 20.
[0246] The certification machine 30 asks for K' by the following count.

[0247]
[Equation 41] K'=tp+f(dp,n)
The certification auxiliary information tp of K' corresponds with the certification information K at a right case.
[0248] A certification machine calculates f (K', r2, m), and compares it with the 2nd term of R1. When both are equal, according to the information m transmitted from the verification machine 20, the internal state corresponding to the right which should be verified is changed. Subsequently, the certification machine 30 searches for the 2nd response indication R2.
[0249]
[Equation 42] R2=(L,f(tp+f(dp,n,L),r,L))
When the certification machine 30 holds the right certification auxiliary information tp, K' is in agreement with the certification information K, and it is [0250].
[Equation 43] R2=(L,f(K,r,L))
It becomes.
[0251] The verification machine 20 calculates tv+f (dv, n), and asks for K. Subsequently, it restricts, when ** [both] and the use limit description L fulfill a service condition in quest of f (K, r) as compared with the 2nd term of R2, and it judges with that in which the certification machine 30 has use rating.
[0252] Although it shall judge whether the use limit description L fulfills a service condition with the verification vessel 20 here, the certification machine 30 may be made to perform.
[0253] The 9th example of [the 9th example] forms the decode section 208 in the verification machine 20 in the 8th example. Drawing 7 shows the configuration of the 9th example and gave the corresponding sign to the corresponding part with drawing 6 in this drawing.
[0254] The information and the verification procedure which are treated in the 9th example are the same as the 8th example. When it judges with a certification machine having use rating, the decode section 208 decodes the information enciphered using the certification information K and K, using a computable value as a key.
[0255] [Example which is the 10th] The 10th example is explained below. This example enables it to manage use hysteresis.
[0256] Drawing 8 shows the configuration of the 10th example and gave the corresponding sign to drawing 7 and a corresponding part in this drawing. In drawing 8 , the hysteresis Management Department 308 is established in the certification machine 30.
[0257] Hereafter, the Challenge Handshake Authentication Protocol of the 10th example is explained.
[0258] This authentication procedure is shown also in drawing 10 . Since each actuation of the 9th of the 5th - an example is included in the 10th example, it can also understand actuation of the 9th of the 5th - an example from drawing 10 .
[0259] In the 10th example, the certification auxiliary information tv on a verification machine and the certification auxiliary information tp on a certification machine are defined as follows.
[0260]
[Equation 44]
tv=K-f(dv,n)
tp=K-f(dp,n,L)
The information and L from which K discriminates the right to which a tropism function and dv should verify certification information and f, and the confidential information of the verification machine 20 and dp should, on the other hand, verify the confidential information of the certification machine 30 and n here are use limit description. The use limit description L is a bit string showing the expiration date.
[0261] The verification machine 20 calculates tv+f (dv, n), and asks for K.
[0262] The 1st trial information C1 sent to the certification machine 30 from the verification machine 20 uses r1 as a random number, and is [0263].
[Equation 45] C1=(n,I,r,s)
It comes out. Here, the information and s which transmit I to a certification machine from a verification machine are [0264].
[Equation 46] s=f(K,I,r)
It is the becoming value.
[0265] The certification machine 30 asks for K' by the following count.

[0266]
[Equation 47] K'=tp+f(dp,n,L)
Subsequently, the certification machine 30 calculates f (K', I, r), and compares it with s. It restricts, when s is in agreement, and the information containing I is stored in the hysteresis attaching part 308.
[0267] The certification machine 30 sends the 2nd trial information C2 to a verification machine.
[0268]
[Equation 48] C2=r2 -- here, r2 is a random number.
[0269] The verification machine 20 calculates tv+f (dv, n), and asks for K. Subsequently, the 1st response indication R1 is searched for by the following count.
[Equation 49] R1=(m,f(K,r2,m))
Here, m is information transmitted to a certification machine from a verification machine. A certification machine asks for K' by the following count.
[0270]
[Equation 50] K'=tp+f(dp,n)
The certification auxiliary information tp of K' corresponds with the certification information K at a right case.
[0271] The certification machine 30 calculates f (K', r2, m), and compares it with the 2nd term of R1. When both are equal, according to the information m transmitted from the verification machine 20, the internal state corresponding to the right which should be verified is changed.
[0272] Subsequently, the certification machine 30 searches for the 2nd response indication R2.
[0273]
[Equation 51] R2=(L,f(tp+f(dp,n,L),r,L))
It is [0274] when the certification machine 30 holds the right certification auxiliary information tp.
[Equation 52] It is set to tp+f(dp, n, L) =K-f(dp, n, L)+f(dp, n, L) =K, the certification information K can be restored, and it is [0275].
[Equation 53] R2=(L,f(K,r,L))
It becomes.
[0276] The verification machine 20 is compared with R2 in quest of f (K, r). It restricts, when ** [both] and L fulfill a service condition, and it judges with that in which the certification machine 30 has use rating.
[0277] Here, although it shall judge whether the use limit description L fulfills a service condition with the verification vessel 20, the certification machine 30 may be made to perform.
[0278] In the above example, although MD5 and SHA were mentioned as an example as a tropism function on the other hand, common use cryptosystems, such as DES, may be used instead.
[0279] Although information used for authentication of a verification machine and the certification of a certification machine having a right was made into the same certification information in the above this example, it supposes that certification information separate about each is used, and you may make it treat suitable information in a certification information attaching part, a confidential information attaching part, and the certification auxiliary Research and Data Processing Department.
[0280] Although especially the thing for which hardware with tamper-proof nature is used is not made into the premise in the above example, unjust risk can be reduced a certification information attaching part, a confidential information attaching part, and by on the other hand protecting the tropism function count section by hardware with tamper-proof nature.
[0281] Although the use rating verification equipment of this invention was used in the above example for control of the propriety of activation of software, it is possible to use as a ticket (ticket) usually used with the various services currently provided with certification auxiliary information in the real world.
[0282] Although the result of on the other hand having subtracted the ******** value for tropism functions from certification information was used as certification auxiliary information in the above example, the exclusive OR for every bit etc. should just be the result of applying the combination of the operation which can be counted backward to certification information.
[0283] [Example of application] Below, the concrete example of application of an example is explained. In addition, below, the thing of certification auxiliary information is called a ticket.
[0284] First, the case where it uses for the access control of software is explained.
[0285] Drawing 16 shows the example which performs the access control of software on a network. In addition,

in drawing 16 , the corresponding sign was given to the corresponding part with drawing 1 . In drawing 16 , the user calculating machine 1000 and the ticket issue calculating machine 2000 are connected in the network 3000. WAN or LAN is sufficient as a network 3000. The predetermined operating system 1002 is installed in hardware 1001, and, as for the user calculating machine 1000, an application program 1003 and the certification program 30 operate on this operating system 1002. The verification program 20 is embedded at the application program 1003. An application program 1003 may be offered with the gestalt of a record medium, is offered on-line, and its potato is good. As for a part of certification program 30, it is desirable to perform on the tamper-proof equipment mounted in the user computer 1000.

[0286] The ticket issue calculating machine 2000 also has hardware 2001 and an operating system 2002, and the ticket issue server 30 operates.

[0287] A user demands issue of the auxiliary information for certification (ticket) of a ticket issue server to use application 1003. This demand is accompanied by a user's identification number and the identification number of application. the ticket issue server 10 -- a user's identification number and the identification number of application -- being based -- respectively -- a user's confidential information and the law of a public key -- a number and certification information are taken out. And certification auxiliary information is calculated and the certification program 20 of the use computer 1000 is passed.

[0288] Henceforth, the certification program 30 and the verification program 20 attest by exchanging the trial information C and a response indication R, and an application program will become available if authentication is successful.

[0289] It is possible to carry out the code of a part of software [at least] by the cryptographic key as the technique of protection of software (application 1003). The cryptographic key of software is set to K and a random number is set to r. For insurance, it is desirable not to contain the key K itself in software. What is necessary is just to inspect whether when not contained in software, the key K itself decodes a part of enciphered software, and it fulfills predetermined conditions.

[0290] The example which uses an example for control of ticket gate equipment next is explained. Drawing 17 shows the ticket gate system by which this example was applied, and the program which realizes the certification machine 30 is installed in IC card 4000 in this drawing. The ticket issue terminal 5000 has a removable IC card, communicates with the ticket issue server 30, and writes certification auxiliary information (ticket) in IC card 4000. A user shows the entrance gate 6000 IC card 4000, when coming in (inserting in a slot), and he attests in the meantime by the verification equipment 10 of the entrance gate 6000 and the certification equipment 20 of IC card 4000 communicating mutually. If authentication is successful, it will enable a user to pass through the entrance gate 6000.

[0291]

[Effect of the Invention] Generally as compared with a public-key-encryption system, the hash is thousands times more nearly high-speed. BruceSchneier, Applied When the MD5 algorithm which calculates a 128-bit digest is performed by the processor made from U.S. Intel (33MHz 486SX, trademark) according to Cryptography (SecondEdition), Wiley, and 1996, 174MB/s can encode. as mentioned above -- according to this writing -- law -- as for the time amount which performs the RSA cryptosystem of number 1024 bit and, and 8 bits of public keys by SPARC2, as for verification, the signature has taken 0.08 seconds for 0.97 seconds. Therefore, it is possible by changing an authentication device into a hash from a public-key-encryption system to reduce computational complexity to 1/thousands, and to raise execution speed.

[0292] As mentioned above, according to the use rating verification equipment of this invention, the access control of software can be performed efficiently. Furthermore, by using certification auxiliary information for a verification machine side, the hardware which can perform an arcade game and various services can be restricted, and the collection and the franchise system of the charge of a license which receive hard can be realized.

[Translation done.]

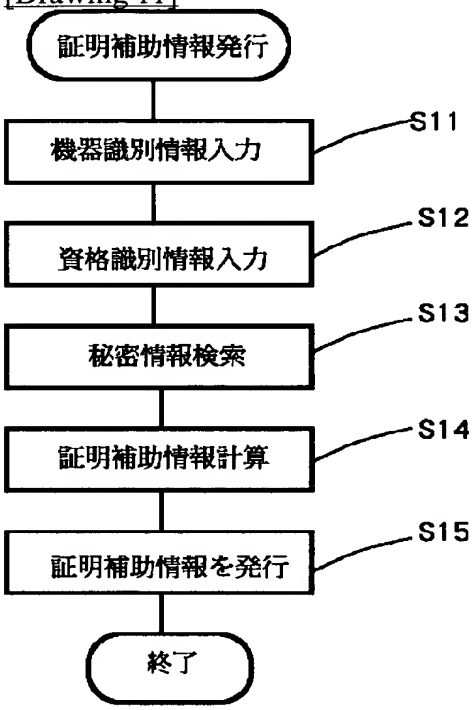
* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

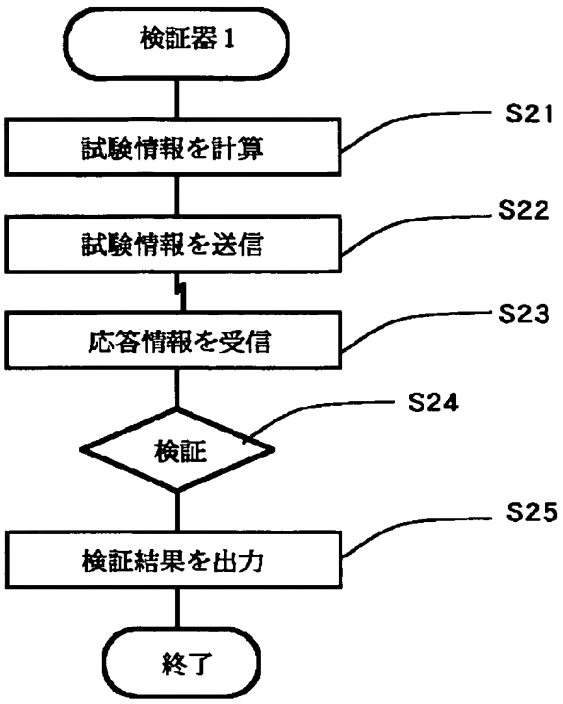
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

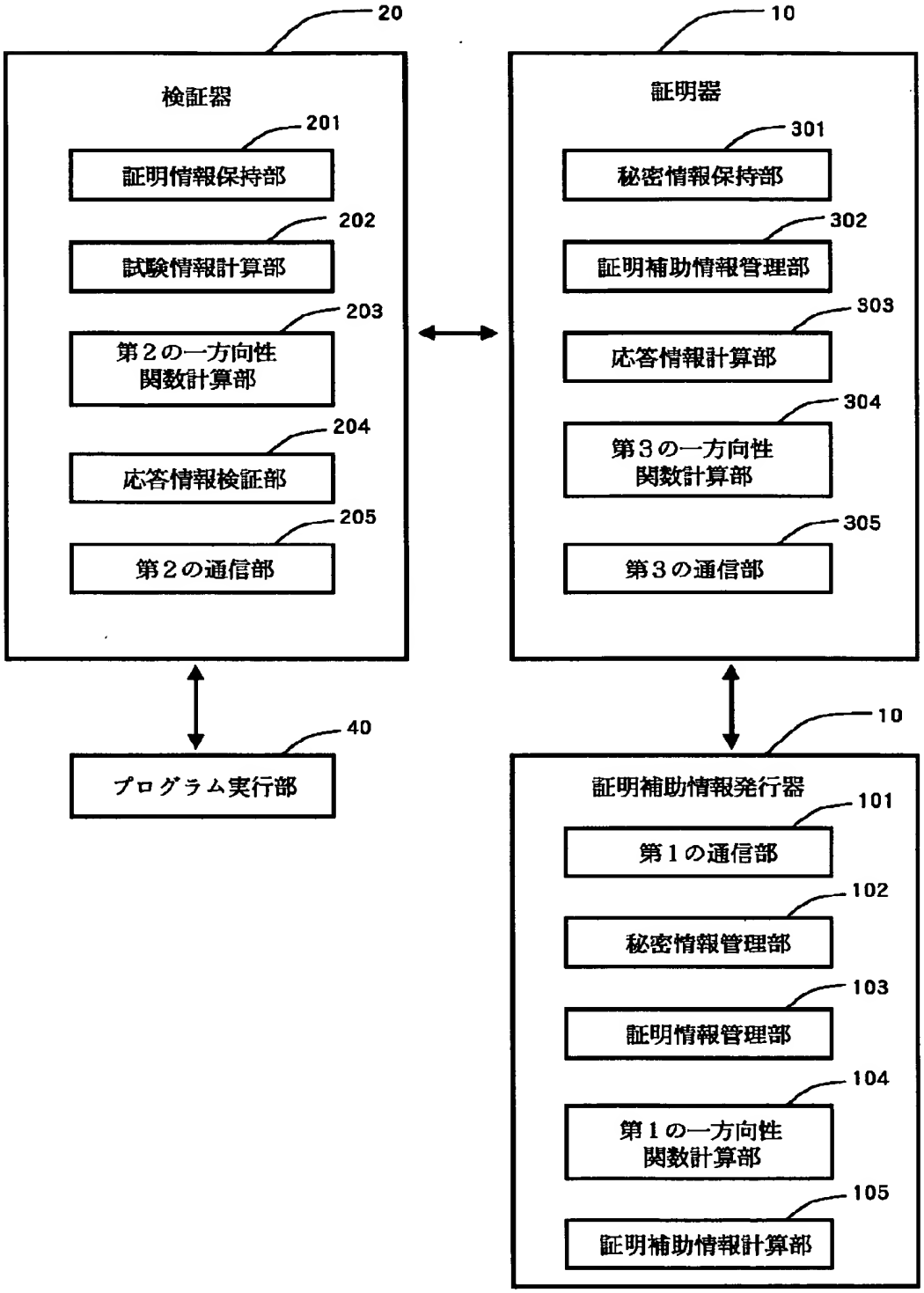
[Drawing 11]



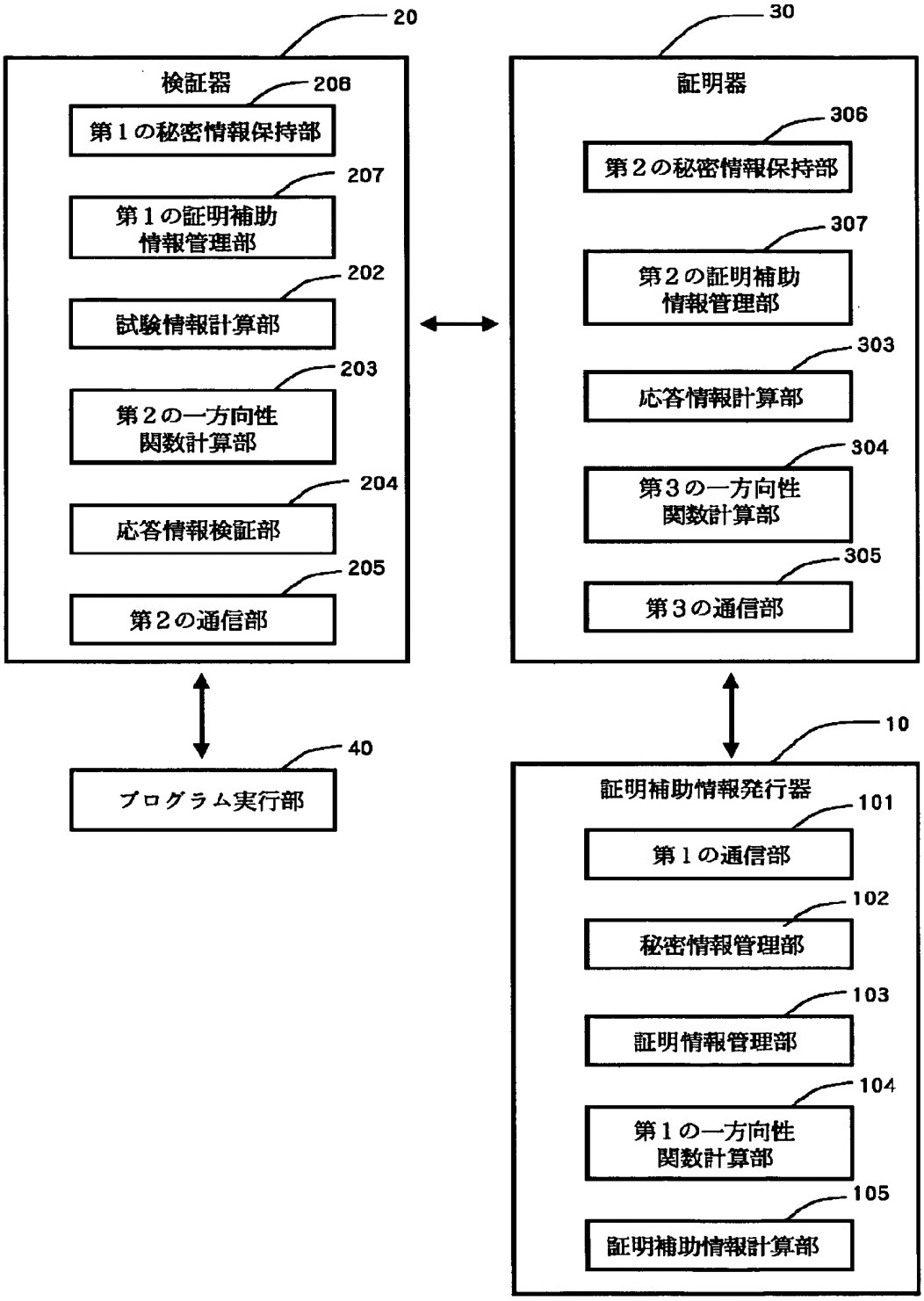
[Drawing 12]


検証器 1
S21
試験情報を計算
S22
試験情報を送信
S23
応答情報を受信
S24
検証
S25
検証結果を出力
終了

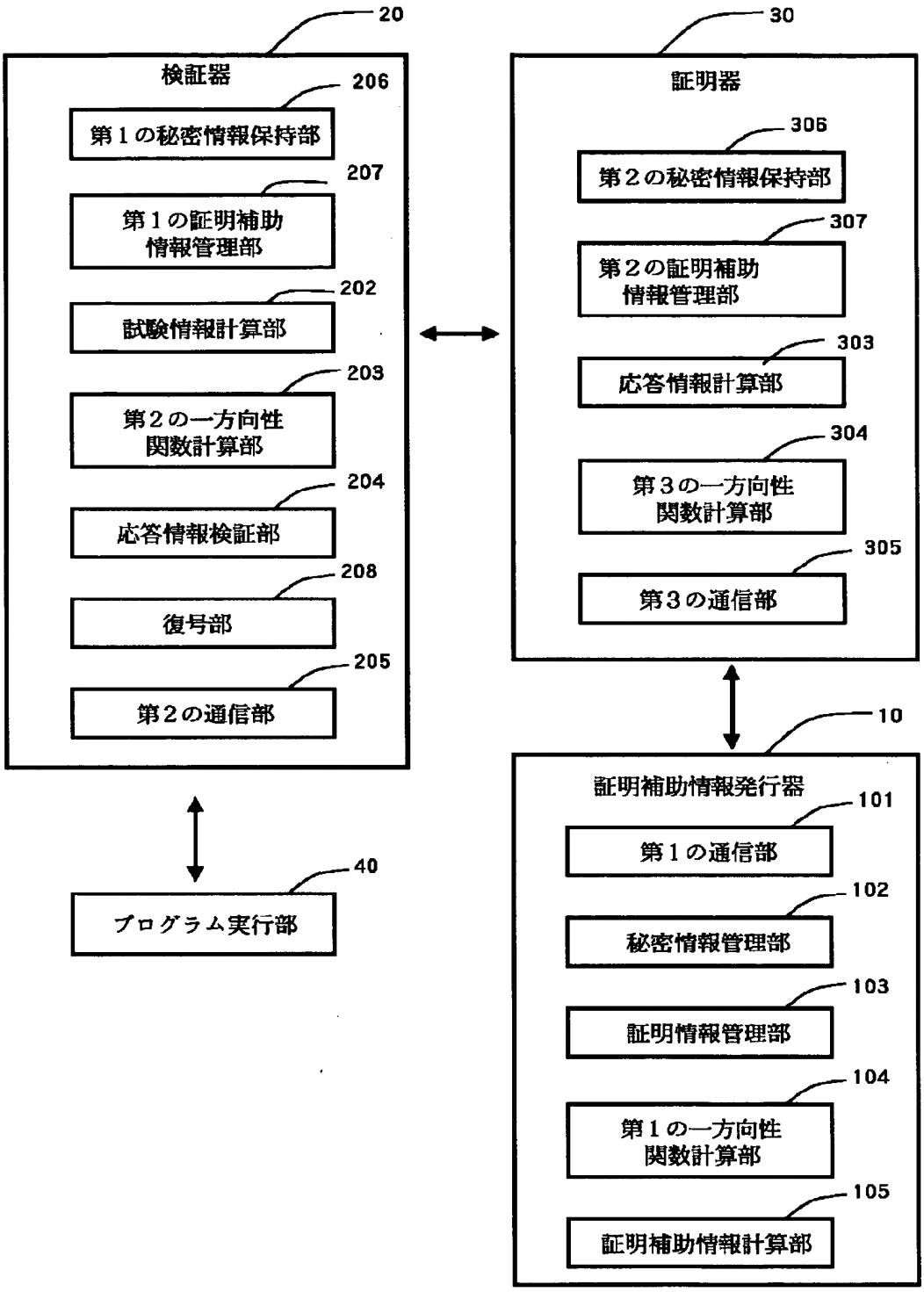
[Drawing 1]


20
検証器
201
証明情報保持部
202
試験情報計算部
203
第２の一方向性
関数計算部
204
応答情報検証部
205
第２の通信部
10
証明器
301
秘密情報保持部
302
証明補助情報管理部
303
応答情報計算部
304
第３の一方向性
関数計算部
305
第３の通信部
40
プログラム実行部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性
関数計算部
105
証明補助情報計算部

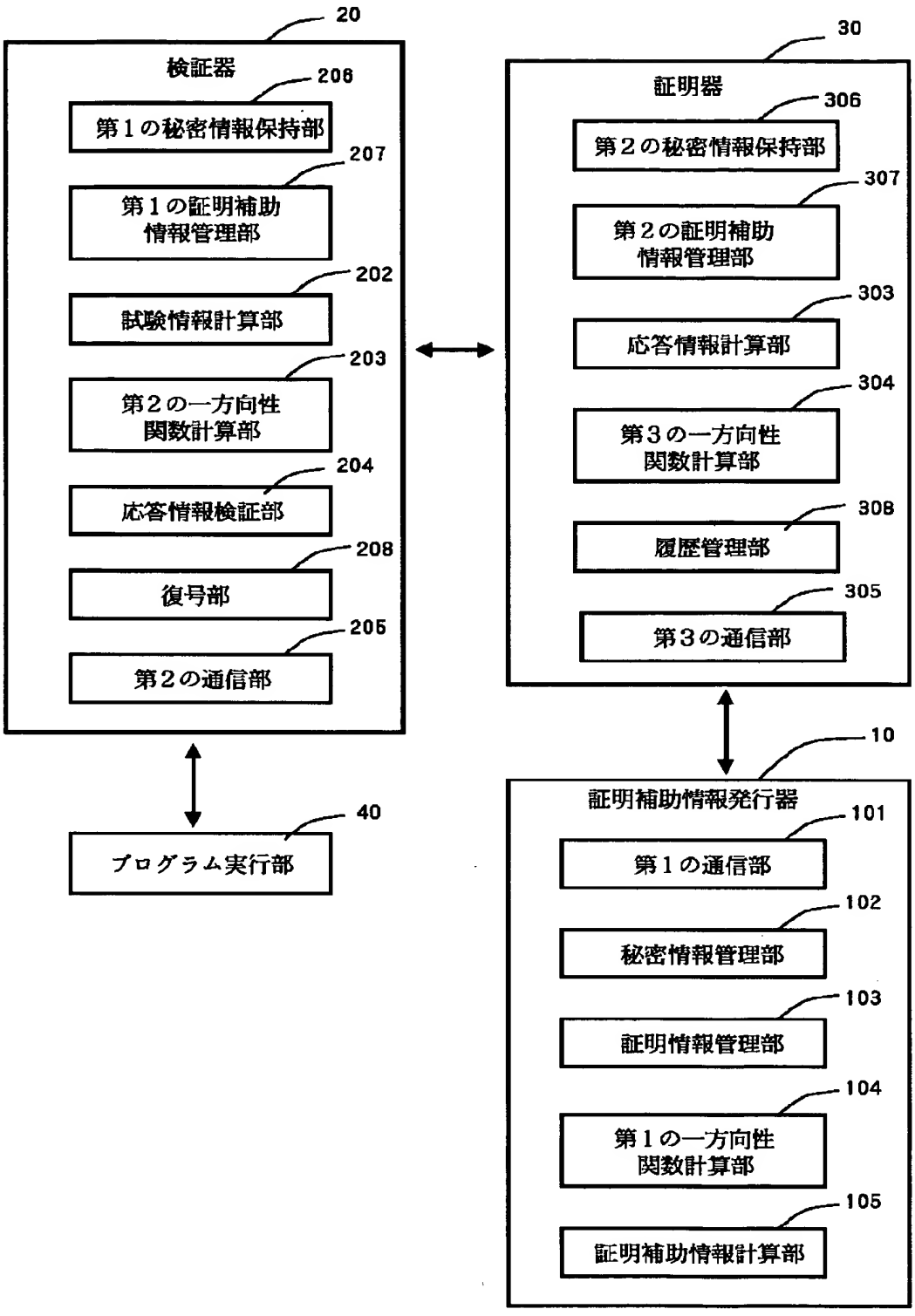
[Drawing 2]


20
検証器
206
第１の秘密情報保持部
207
第１の証明補助
情報管理部
202
試験情報計算部
203
第２の一方向性
関数計算部
204
応答情報検証部
205
第２の通信部
40
プログラム実行部
30
証明器
306
第２の秘密情報保持部
307
第２の証明補助
情報管理部
303
応答情報計算部
304
第３の一方向性
関数計算部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性
関数計算部
105
証明補助情報計算部

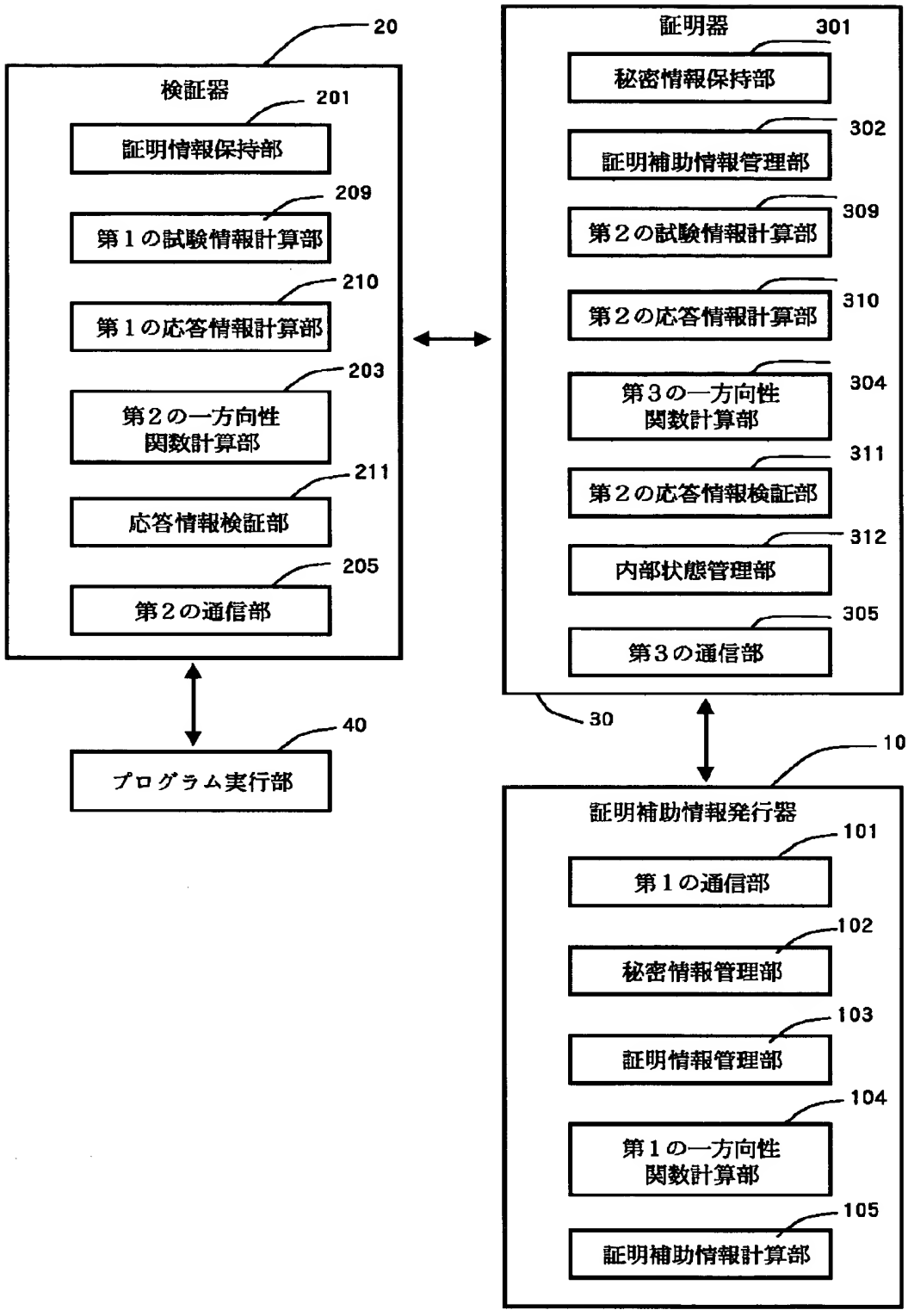
[Drawing 3]


20
検証器
206
第１の秘密情報保持部
207
第１の証明補助
情報管理部
202
試験情報計算部
203
第２の一方向性
関数計算部
204
応答情報検証部
208
復号部
205
第２の通信部
40
プログラム実行部
30
証明器
306
第２の秘密情報保持部
307
第２の証明補助
情報管理部
303
応答情報計算部
304
第３の一方向性
関数計算部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性
関数計算部
105
証明補助情報計算部

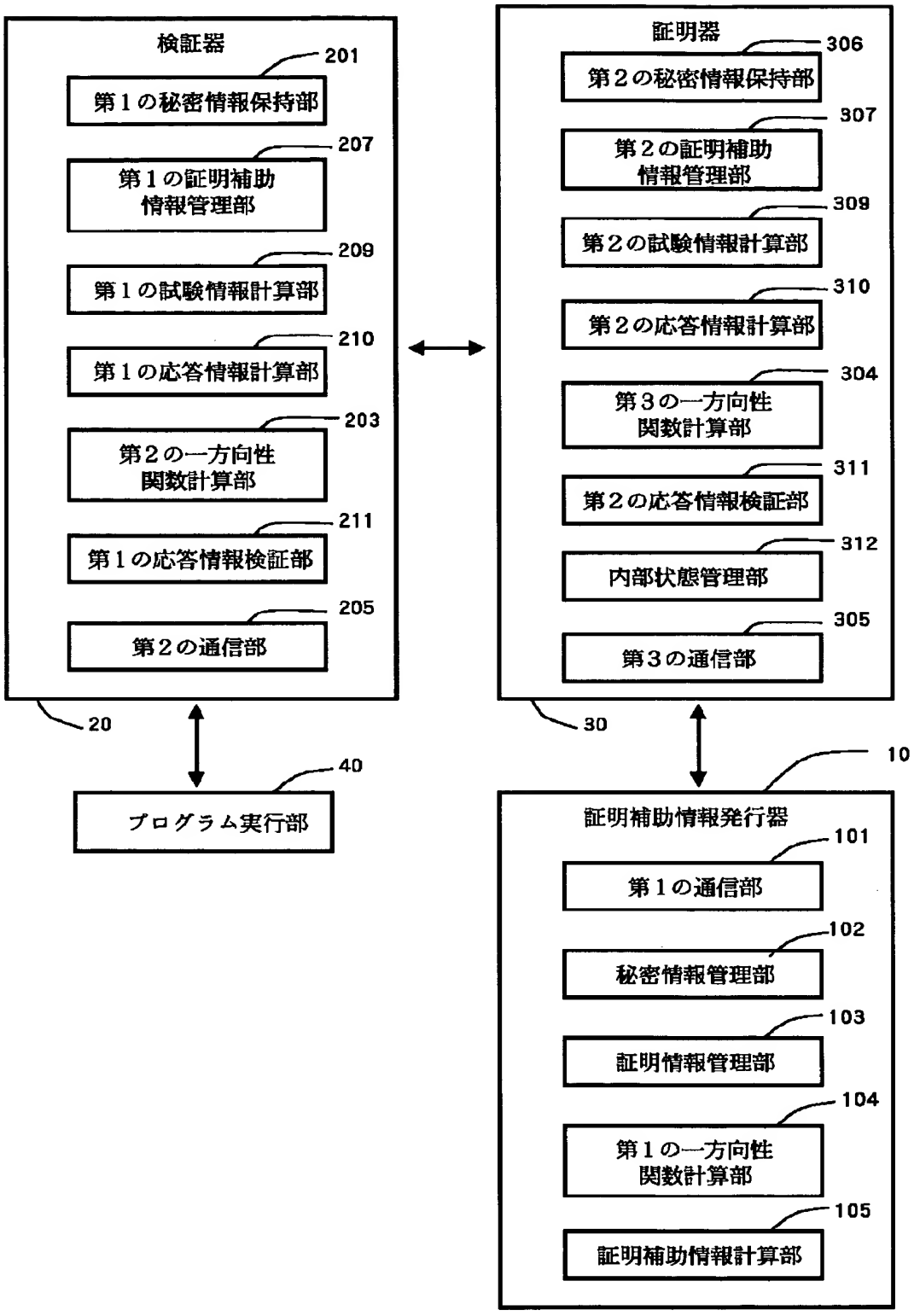
[Drawing 4]


20
検証器
206
第１の秘密情報保持部
207
第１の証明補助
情報管理部
202
試験情報計算部
203
第２の一方向性
関数計算部
204
応答情報検証部
208
復号部
205
第２の通信部
40
プログラム実行部
30
証明器
306
第２の秘密情報保持部
307
第２の証明補助
情報管理部
303
応答情報計算部
304
第３の一方向性
関数計算部
308
履歴管理部
305
第３の通信部
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性
関数計算部
105
証明補助情報計算部

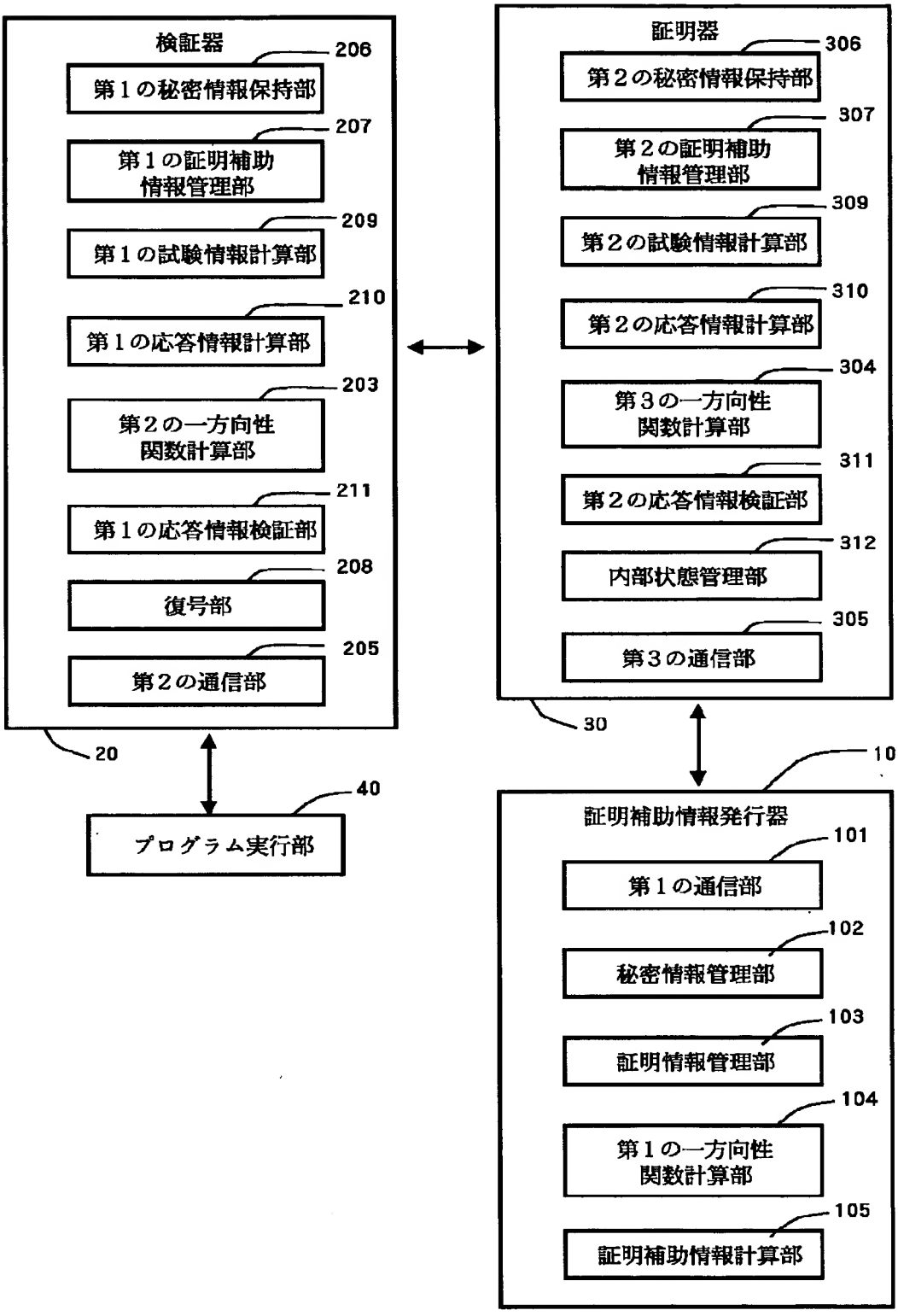
[Drawing 5]


20
検証器
201
証明情報保持部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
応答情報検証部
205
第２の通信部
40
プログラム実行部
証明器
301
秘密情報保持部
302
証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

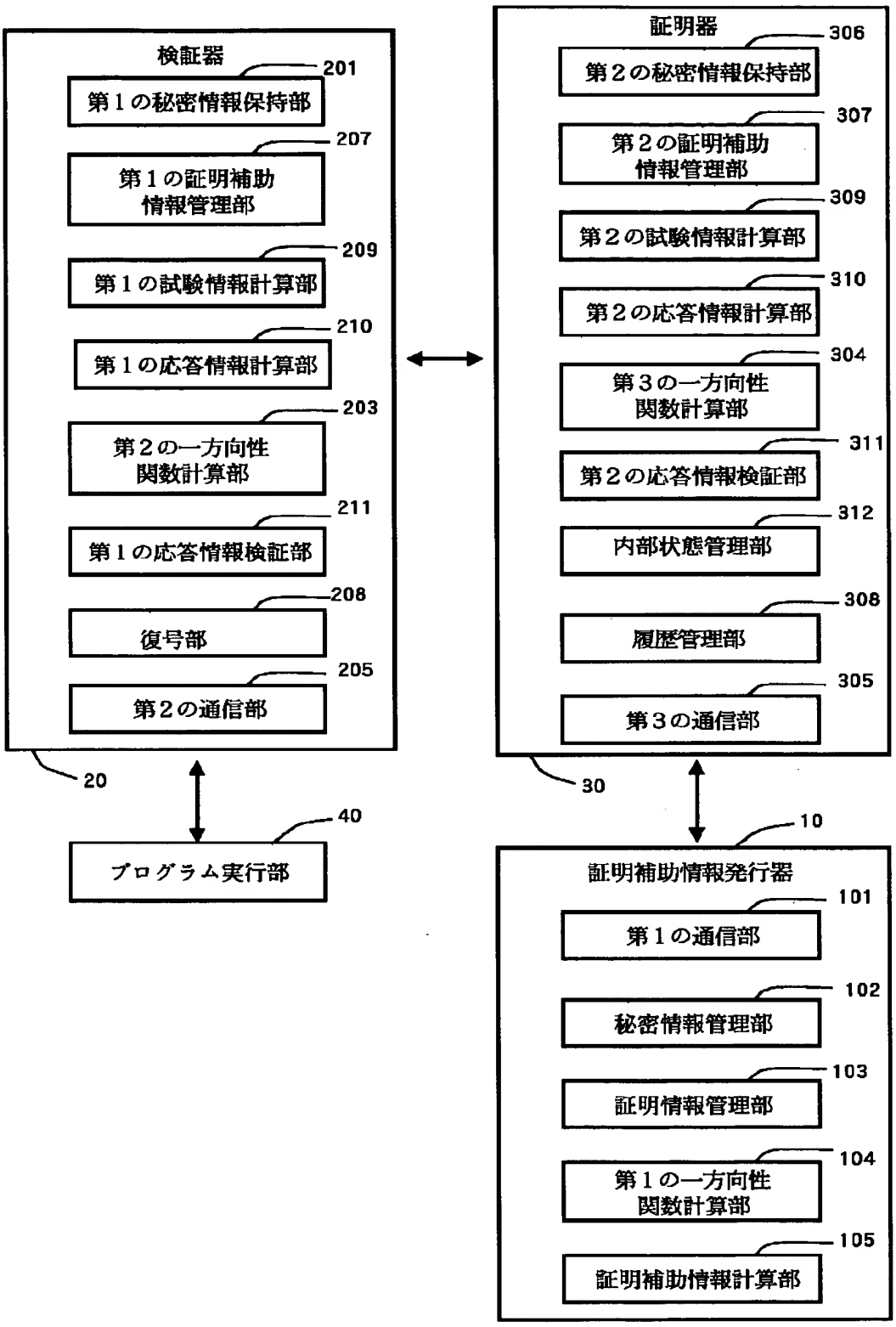
[Drawing 6]


検証器
201
第１の秘密情報保持部
207
第１の証明補助情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
第１の応答情報検証部
205
第２の通信部
20
40
プログラム実行部
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

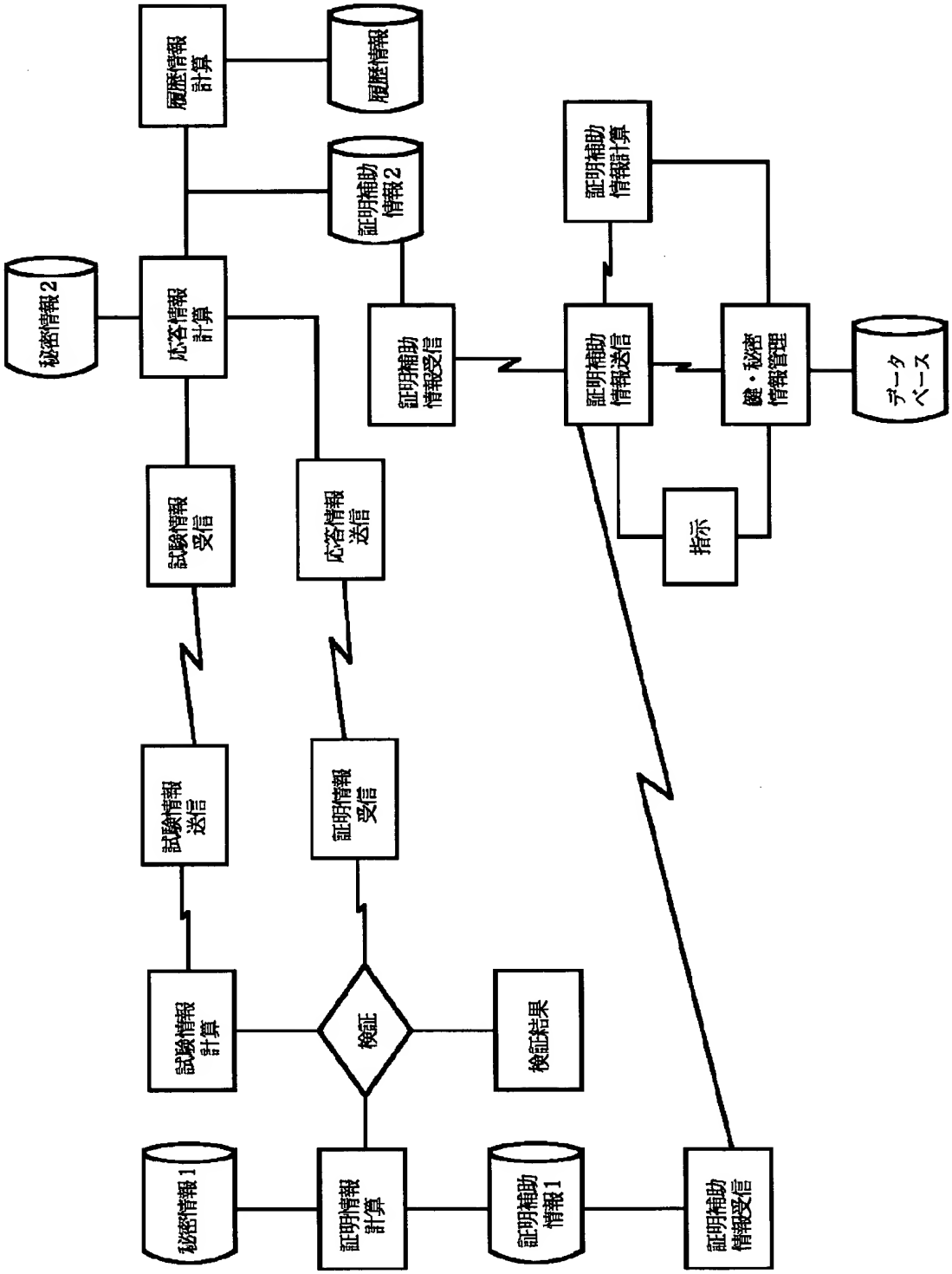
[Drawing 7]


検証器
206
第１の秘密情報保持部
207
第１の証明補助情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性関数計算部
211
第１の応答情報検証部
208
復号部
205
第２の通信部
20
40
プログラム実行部
証明器
306
第２の秘密情報保持部
307
第２の証明補助情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性関数計算部
311
第２の応答情報検証部
312
内部状態管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性関数計算部
105
証明補助情報計算部

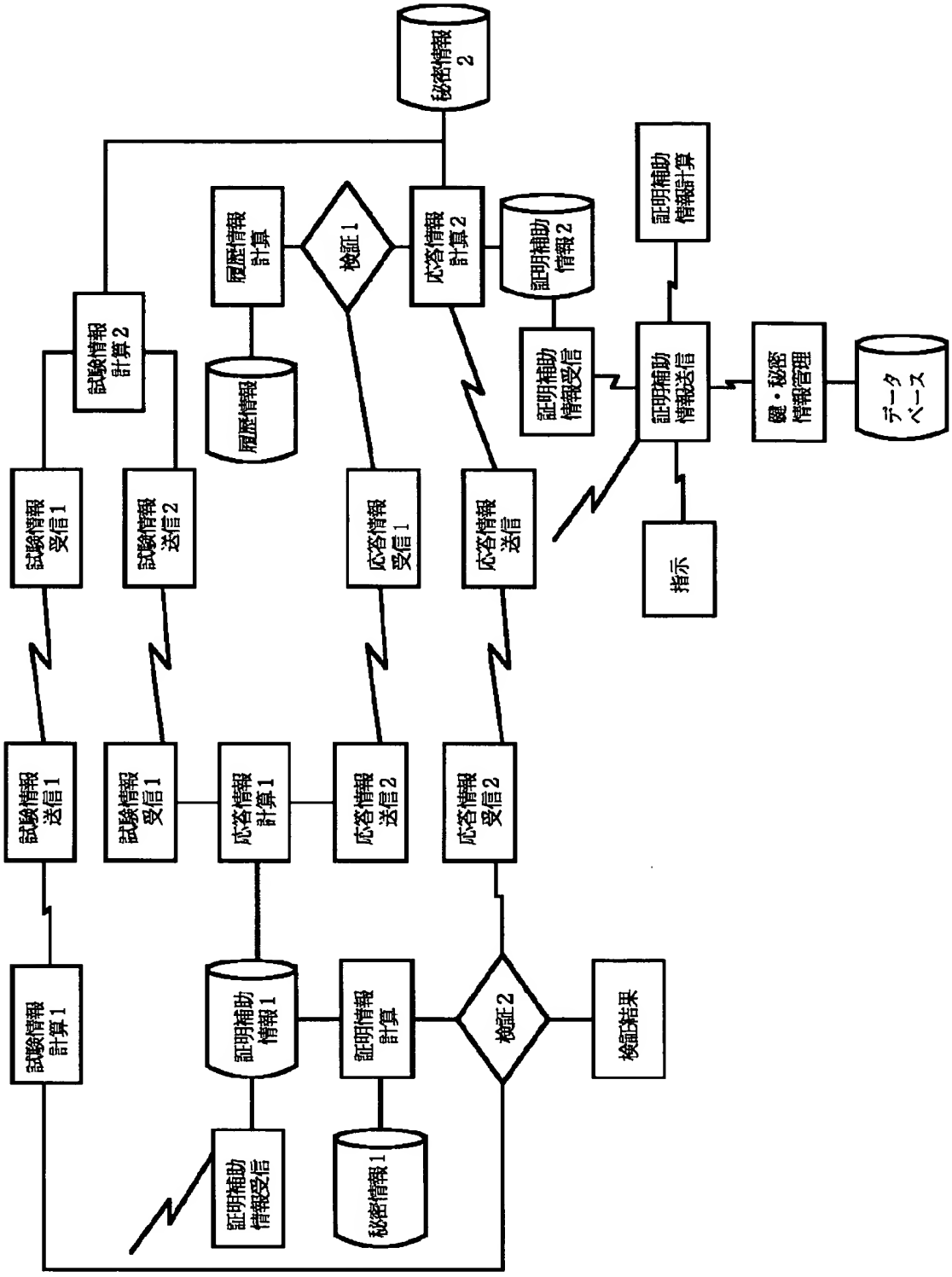
[Drawing 8]


検証器
201
第１の秘密情報保持部
207
第１の証明補助
情報管理部
209
第１の試験情報計算部
210
第１の応答情報計算部
203
第２の一方向性
関数計算部
211
第１の応答情報検証部
208
復号部
205
第２の通信部
20
40
プログラム実行部
証明器
306
第２の秘密情報保持部
307
第２の証明補助
情報管理部
309
第２の試験情報計算部
310
第２の応答情報計算部
304
第３の一方向性
関数計算部
311
第２の応答情報検証部
312
内部状態管理部
308
履歴管理部
305
第３の通信部
30
10
証明補助情報発行器
101
第１の通信部
102
秘密情報管理部
103
証明情報管理部
104
第１の一方向性
関数計算部
105
証明補助情報計算部

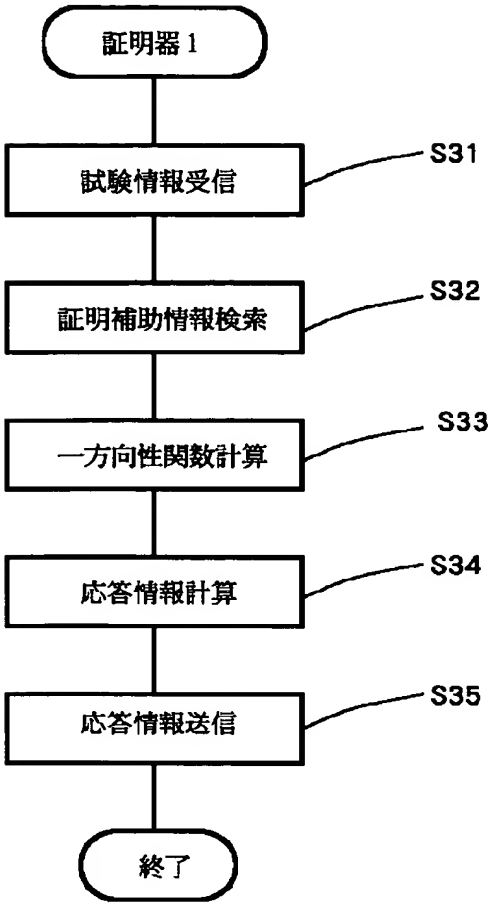
[Drawing 9]


履歴情報計算
履歴情報
証明補助情報2
証明補助情報計算
秘密情報2
応答情報計算
証明補助情報受信
証明補助情報送信
鍵・秘密情報管理
データベース
試験情報受信
応答情報送信
指示
試験情報送信
証明情報受信
試験情報計算
検証
検証結果
秘密情報1
証明情報計算
証明補助情報1
証明補助情報受信

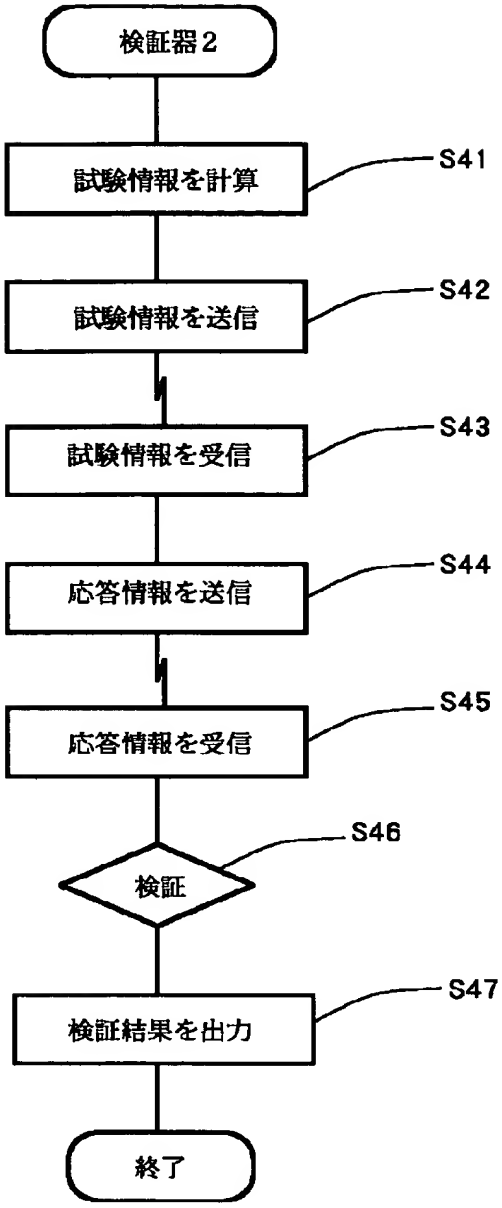
[Drawing 10]


秘密情報2
履歴情報計算
検証1
応答情報計算2
証明補助情報2
証明補助情報計算
試験情報計算2
履歴情報
証明補助情報受信
証明補助情報送信
鍵・秘密情報管理
データベース
試験情報受信1
試験情報送信2
応答情報受信1
応答情報送信
指示
試験情報送信1
試験情報受信1
応答情報計算1
応答情報送信2
応答情報受信2
試験情報計算1
証明補助情報1
証明情報計算
検証2
検証結果
証明補助情報受信
秘密情報1

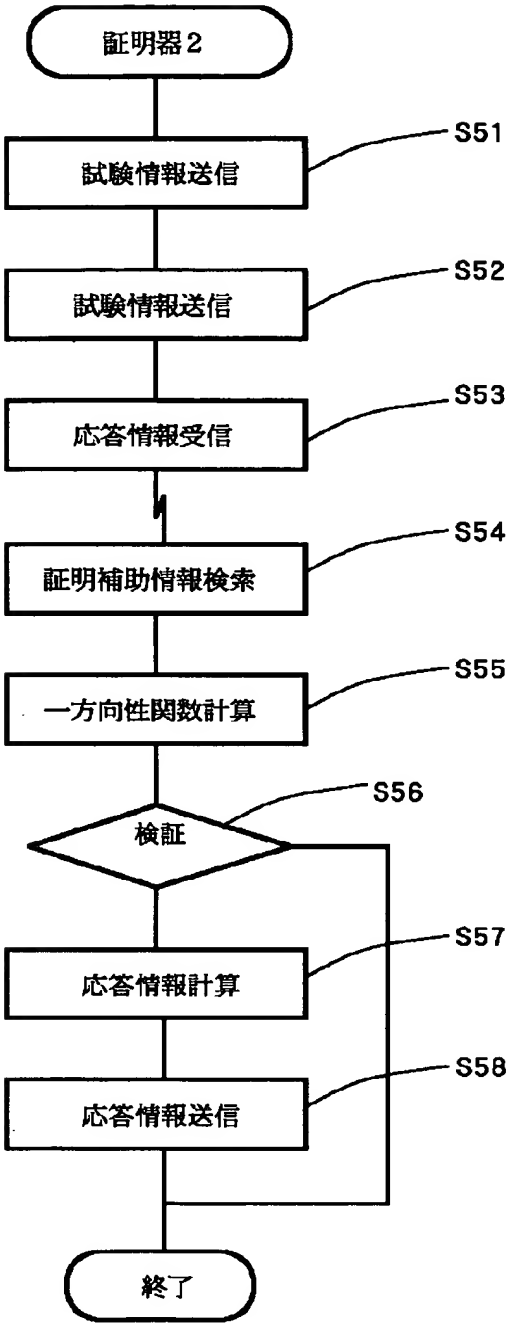
[Drawing 13]


証明器 1
試験情報受信
S31
証明補助情報検索
S32
一方向性関数計算
S33
応答情報計算
S34
応答情報送信
S35
終了

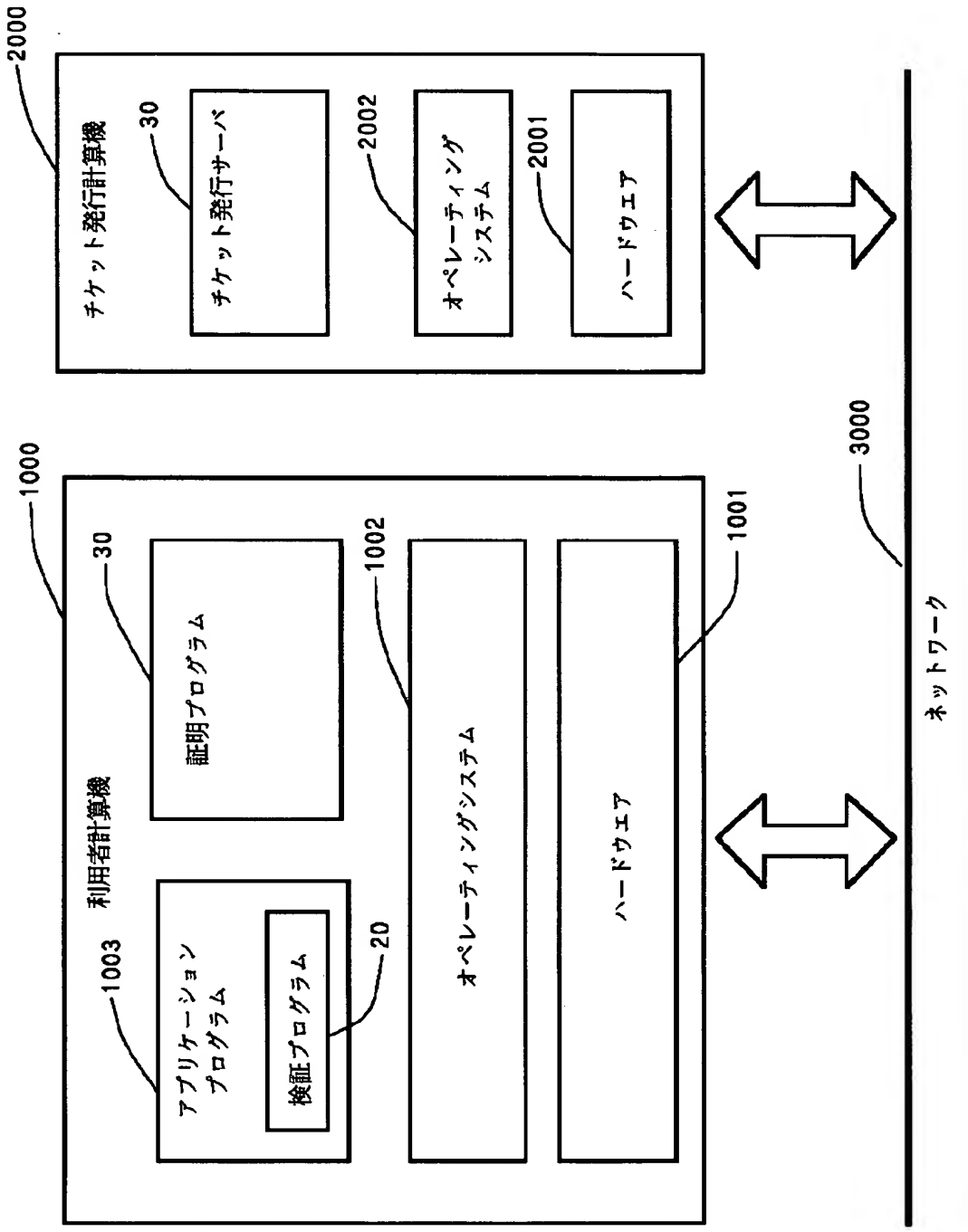
[Drawing 14]


検証器2
試験情報を計算
S41
試験情報を送信
S42
試験情報を受信
S43
応答情報を送信
S44
応答情報を受信
S45
検証
S46
検証結果を出力
S47
終了

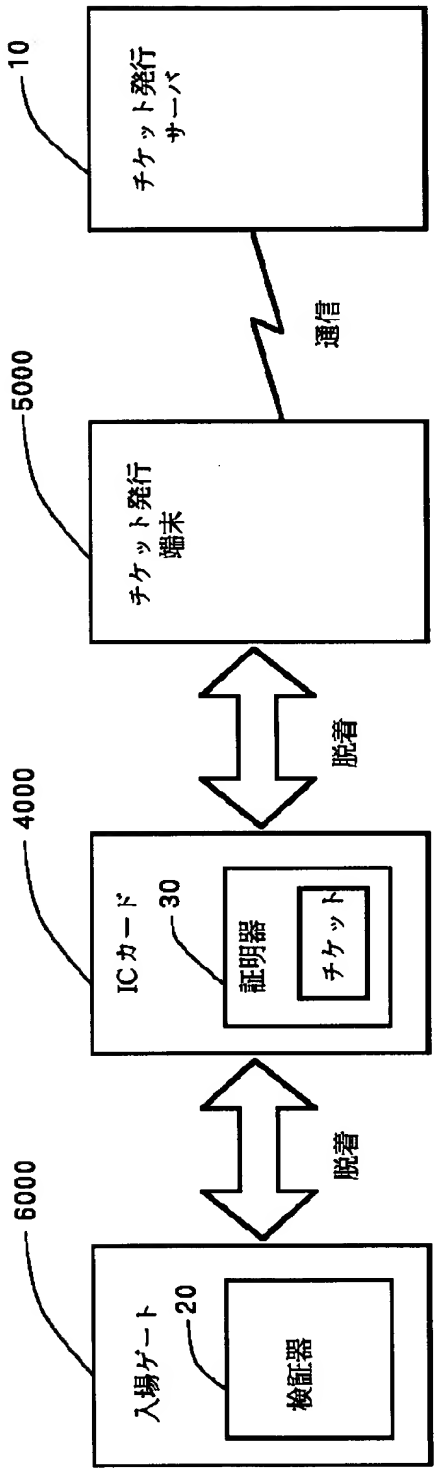
[Drawing 15]


証明器2
S51
試験情報送信
S52
試験情報送信
S53
応答情報受信
S54
証明補助情報検索
S55
一方向性関数計算
S56
検証
S57
応答情報計算
S58
応答情報送信
終了

[Drawing 16]


2000
チケット発行計算機
30
チケット発行サーバ
2002
オペレーティングシステム
2001
ハードウエア
3000
ネットワーク
1000
利用者計算機
30
証明プログラム
1002
オペレーティングシステム
1001
ハードウエア
1003
アプリケーションプログラム
20
検証プログラム

[Drawing 17]



[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CORRECTION OR AMENDMENT

[Kind of official gazette] Printing of amendment by the convention of 2 of Article 17 of Patent Law
[Section partition] The 3rd partition of the 7th section
[Publication date] January 17, Heisei 15 (2003. 1.17)

[Publication No.] JP,11-234262,A
[Date of Publication] August 27, Heisei 11 (1999. 8.27)
[Annual volume number] Open patent official report 11-2343
[Application number] Japanese Patent Application No. 10-27326
[The 7th edition of International Patent Classification]

H04L 9/32
G06F 9/06 550

G06K 19/10
G09C 1/00 640
660

[FI]

H04L 9/00 675 B
G06F 9/06 550 G
550 C
G09C 1/00 640 E
660 D
G06K 19/00 R

[Procedure revision]
[Filing Date] October 17, Heisei 14 (2002. 10.17)
[Procedure amendment 1]
[Document to be Amended] Specification
[Item(s) to be Amended] Claim
[Method of Amendment] Modification
[Proposed Amendment]
[Claim(s)]
[Claim 1] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section,
Said certification auxiliary information issue section,
A certification information management means to manage the certification information used in the case of authentication of use rating,
The confidential information management tool which manages secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means to the confidential information which said confidential information management tool manages at least,

The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand,
It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information,
Said verification section,
A certification information maintenance means to hold certification information,
A trial information count means to calculate trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,
The certification information which said certification information maintenance means holds, and a response indication verification means to inspect whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of trial information,
It has the 2nd means of communications which transmits and receives information in process of authentication of use rating,
Said certification section,
A confidential information maintenance means to hold secret information,
A certification auxiliary information management means to manage the certification auxiliary information that it uses for count of a response indication,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,
It is said 3rd response indication count means to calculate a response indication by on the other hand making a tropism function count means act, to the value acquired based on a part or all of trial information, the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages,
Use rating verification equipment characterized by having the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 2] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section,
Said certification auxiliary information issue section,
A certification information management means to manage the certification information used in the case of authentication of use rating,
The confidential information management tool which manages secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means to the confidential information which said confidential information management tool manages at least,
The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand,
It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information,
Said verification section,
The 1st confidential information maintenance means holding secret information,
The 1st certification auxiliary information management means which manages certification auxiliary information,
A trial information count means to calculate trial information,
On the other hand, the 2nd to which asking for an inverse function applies a directivity function difficult in computational complexity at least is a tropism function count means,
The confidential information which said 1st confidential information maintenance means holds, and a response indication verification means to inspect whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of

trial information,
It has the 2nd means of communications which transmits and receives information in process of authentication of use rating,
Said certification section,
The 2nd confidential information maintenance means holding secret information,
The 2nd certification auxiliary information management means which manages the certification auxiliary information that it uses for count of a response indication,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,
It is said 3rd response indication count means to calculate a response indication by on the other hand making a tropism function count means act, to the value acquired based on a part or all of trial information, the confidential information which said 2nd confidential information maintenance means holds, and the certification auxiliary information which said 2nd certification auxiliary information management means manages,
Use rating verification equipment characterized by having the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 3] It is use rating verification equipment of claim 1 thru/or claim 2,
Said certification information management means is combined with certification information, and manages the use limit description which is the information which shows use conditions,
Said certification auxiliary information management means is combined with certification auxiliary information, and manages use limit description,
Use rating verification equipment characterized by including use limit description in count of the response indication generated in the certification auxiliary information that it uses in said certification section, and said certification section.
[Claim 4] Use rating verification equipment characterized by decoding information, using the value acquired from certification information or certification information as a decode key of said decode means when it judges with it being use rating verification equipment of claim 1 thru/or claim 3, and having a decode means, and there being use rating.
[Claim 5] It is use rating verification equipment have the hysteresis management tool which is use rating verification equipment of claim 1 thru/or claim 4, and manages the hysteresis at the time of use rating verification, and combine with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information-management means manage transfer information, and carry out that trial information stores said transfer information to a hysteresis management tool at the time of use rating verification including transfer information further as the description.
[Claim 6] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section,
Said certification auxiliary information issue section,
A certification information management means to manage the certification information used in the case of authentication of use rating,
The confidential information management tool which manages secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means to the confidential information which said confidential information management tool manages at least,
The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand,
It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information,
Said verification section,
A certification information maintenance means to hold certification information,
The 1st trial information count means which calculates the 1st trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least]

which applies a tropism function on the other hand is a tropism function count means,
It is said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and calculates the 1st response indication to the 2nd trial information which received,
The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information,
It has the 2nd means of communications which transmits and receives information in process of authentication of use rating,
Said certification section,
A confidential information maintenance means to hold secret information,
A certification auxiliary information management means to manage the certification auxiliary information that it uses for count of a response indication,
The internal-state management tool which manages the internal state corresponding to certification auxiliary information,
The 2nd trial information count means which calculates trial information,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,
It is said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act to the value acquired based on a part or all of the received information, the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages,
The 2nd trial information count means which calculates the 2nd trial information,
Whether the 3rd [said] result on which the tropism function count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of the 1st response indication and the 2nd trial information, the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages, and the 2nd response indication verification means to inspect,
Use rating verification equipment characterized by having the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 7] In the use rating verification equipment which verifies use rating including the certification auxiliary information issue section, the verification section, and the certification section,
Said certification auxiliary information issue section,
A certification information management means to manage the certification information used in the case of authentication of use rating,
The confidential information management tool which manages secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means to the confidential information which said confidential information management tool manages at least,
The confidential information which said confidential information management tool manages, and said 1st certification auxiliary information count means to calculate certification auxiliary information based on the count result of a tropism function count means on the other hand,
It has the 1st means of communications which transmits and receives information in process of count of certification auxiliary information,
Said verification section,
The 1st confidential information maintenance means holding secret information,
The 1st certification auxiliary information management means which manages certification auxiliary information,
The 1st trial information count means which calculates the 1st trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,

It is said 2nd response indication count means [1st] which a tropism function count means is made to act on the other hand, and calculates the 1st response indication to the 2nd trial information which received,
The 1st response indication verification means which inspects whether the 2nd [said] result on which the tropism count means was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information which said certification information maintenance means holds, and the 1st trial information,
It has the 2nd means of communications which transmits and receives information in process of authentication of use rating,
Said certification section,
The 2nd confidential information maintenance means holding secret information,
The 2nd certification auxiliary information management means which manages the certification auxiliary information that it uses for creation of a response indication,
The internal-state management tool which manages the internal state corresponding to certification auxiliary information,
The 2nd trial information count means which calculates trial information,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count means,
It is said 3rd response indication count means [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count means act to the value acquired based on a part or all of the received information, the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages,
The 2nd trial information count means which calculates the 2nd trial information,
Whether the 3rd [said] result on which the tropism function count means was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of the 1st response indication and the 2nd trial information, the confidential information which said confidential information maintenance means holds, and the certification auxiliary information which said certification auxiliary information management means manages, and the 2nd response indication verification means to inspect,
Use rating verification equipment by which it is characterized [which has the 3rd means of communications which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count].
[Claim 8] It is use rating verification equipment carry out containing use limit description in count of the response indication generated in the certification auxiliary information are use rating verification equipment of claim 6 thru/or claim 7, combine with certification information and a certification information-management means manages the use limit description which is the information which shows use conditions, and combine with certification auxiliary information, manage a certification auxiliary information-management means and use limit description, and use at the certification section, and the certification section as the description.
[Claim 9] Use rating verification equipment characterized by decoding information, using the value acquired from certification information or certification information as a decode key of said decode means when it judges with it being use rating verification equipment of claim 6 thru/or claim 8, and having a decode means, and there being use rating.
[Claim 10] It is use rating verification equipment have the hysteresis management tool which is use rating verification equipment of claim 6 thru/or claim 9, and manages the hysteresis at the time of use rating verification, and combine with certification information or certification auxiliary information, and a certification information maintenance means or the 1st certification auxiliary information-management means manage transfer information, and carry out that trial information stores said transfer information to a hysteresis management tool at the time of use rating verification including transfer information further as the description.
[Claim 11] In the use rating verification approach of verifying use rating including a certification auxiliary information issue step, a verification step, and a certification step,
Said certification auxiliary information issue step,
The certification information maintenance substep holding the certification information used in the case of authentication of use rating,
The confidential information maintenance substep holding secret information,

For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep to the confidential information held by said confidential information maintenance substep at least,
The confidential information held by said confidential information maintenance substep, and said 1st certification auxiliary information count substep which calculates certification auxiliary information based on the count result of a tropism function count substep on the other hand,
It has the 1st communication link substep which transmits and receives information in process of count of certification auxiliary information,
Said verification step,
The certification information maintenance substep holding certification information,
The trial information count substep which calculates trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
The certification information held by said certification information maintenance substep, and the response indication verification substep which inspects whether the 2nd [said] result on which the tropism count substep was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of trial information,
It has the 2nd communication link substep which transmits and receives information in process of authentication of use rating,
Said certification step,
The confidential information maintenance substep holding secret information,
The certification auxiliary information maintenance substep holding the certification auxiliary information that it uses for count of a response indication,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
It is said 3rd response indication count substep which calculates a response indication by on the other hand making a tropism function count substep act to the value acquired based on a part or all of trial information, the confidential information held by said confidential information maintenance substep, and the certification auxiliary information held by said certification auxiliary information maintenance substep,
The use rating verification approach characterized by having the 3rd communication link substep which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 12] In the use rating verification approach of verifying use rating including a certification auxiliary information issue step, a verification step, and a certification step,
Said certification auxiliary information issue step,
The certification information maintenance substep holding the certification information used in the case of authentication of use rating,
The confidential information maintenance substep holding secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep to the confidential information held by said confidential information maintenance substep at least,
The confidential information held by said confidential information maintenance substep, and said 1st certification auxiliary information count substep which calculates certification auxiliary information based on the count result of a tropism function count substep on the other hand,
It has the 1st communication link substep which transmits and receives information in process of count of certification auxiliary information,
Said verification step,
The certification information maintenance substep holding certification information,
The 1st trial information count substep which calculates the 1st trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
It is said 2nd response indication count substep [1st] which a tropism function count substep is made to act on the other hand, and calculates the 1st response indication to the 2nd trial information which received,

The 1st response indication verification substep which inspects whether the 2nd [said] result on which the tropism count substep was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information held by said certification information maintenance substep, and the 1st trial information,
It has the 2nd communication link substep which transmits and receives information in process of authentication of use rating, and is said certification step,
The confidential information maintenance substep holding secret information,
The certification auxiliary information maintenance substep holding the certification auxiliary information that it uses for count of a response indication,
The internal-state maintenance substep holding the internal state corresponding to certification auxiliary information,
The 2nd trial information count substep which calculates trial information,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
It is said 3rd response indication count substep [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count substep act to the value acquired based on informational a part or informational all that was received, the confidential information held by said confidential information maintenance substep, and the certification auxiliary information held by said certification auxiliary information maintenance substep,
The 2nd trial information count substep which calculates the 2nd trial information,
Whether the 3rd [said] result on which the tropism function count substep was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of the 1st response indication and the 2nd trial information, the confidential information held by said confidential information maintenance substep, and the certification auxiliary information held by said certification auxiliary information maintenance substep, and the 2nd response indication verification substep to inspect,
The use rating verification approach characterized by having the 3rd communication link substep which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count.
[Claim 13] In the use rating verification approach of verifying use rating including a certification auxiliary information issue step, a verification step, and a certification step,
Said certification auxiliary information issue step,
The certification information maintenance substep holding the certification information used in the case of authentication of use rating,
The confidential information maintenance substep holding secret information,
For asking for an inverse function, on the other hand, the 1st [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep to the confidential information held by said confidential information maintenance substep at least,
The confidential information held by said confidential information maintenance substep, and said 1st certification auxiliary information count substep which calculates certification auxiliary information based on the count result of a tropism function count substep on the other hand,
It has the 1st communication link substep which transmits and receives information in process of count of certification auxiliary information,
Said verification step,
The 1st confidential information maintenance substep holding secret information,
The 1st certification auxiliary information maintenance substep holding certification auxiliary information,
The 1st trial information count substep which calculates the 1st trial information,
For asking for an inverse function, on the other hand, the 2nd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
It is said 2nd response indication count substep [1st] which a tropism function count substep is made to act on the other hand, and calculates the 1st response indication to the 2nd trial information which received,
The 1st response indication verification substep which inspects whether the 2nd [said] result on which the tropism count substep was made to act on the other hand, and the 2nd response indication are equal to the value acquired based on a part or all of the certification information held by said certification information

maintenance substep, and the 1st trial information,
It has the 2nd communication link substep which transmits and receives information in process of authentication of use rating,
Said certification step,
The 2nd confidential information maintenance substep holding secret information,
The 2nd certification auxiliary information maintenance substep holding the certification auxiliary information that it uses for creation of a response indication,
The internal-state maintenance substep holding the internal state corresponding to certification auxiliary information,
The 2nd trial information count substep which calculates trial information,
For asking for an inverse function, on the other hand, the 3rd [difficult in computational complexity at least] which applies a tropism function on the other hand is a tropism function count substep,
It is said 3rd response indication count substep [2nd] which calculates the 2nd response indication by on the other hand making a tropism function count substep act to the value acquired based on informational a part or informational all that was received, the confidential information held by said confidential information maintenance substep, and the certification auxiliary information held by said certification auxiliary information maintenance substep,
The 2nd trial information count substep which calculates the 2nd trial information,
Whether the 3rd [said] result on which the tropism function count substep was made to act on the other hand, and a response indication are equal to the value acquired based on a part or all of the 1st response indication and the 2nd trial information, the confidential information held by said confidential information maintenance substep, and the certification auxiliary information held by said certification auxiliary information maintenance substep, and the 2nd response indication verification substep to inspect,
The use rating verification approach by which it is characterized [which has the 3rd communication link substep which transmits and receives information in process of the process of authentication of use rating, and certification auxiliary information count].

[Translation done.]